August 10, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-ninth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at [redacted] if there are any questions.

Invoice 39:

Period	Months	Rate	Cost
06/17/2011 - 07/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG08102011

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: August 10, 2011

This report documents progress in July 2011 on contract BBGCON1807S6441 between BBG and The Tor Project.

New releases, new hires, new funding

New Releases

1. On July 7, we released Torbutton 1.4.0. The addon has been disabled on addons.mozilla.org. Our URL is now canonical.

   This release features support for Firefox 5.0, and has been tested against the vanilla release for basic functionality. However, it has not been audited for Network Isolation, State Separation, Tor Undiscoverability or Interoperability issues[1] due to toggling under Firefox 5.

   If you desire Torbutton functionality with Firefox 4/5, we recommend you download the Tor Browser Bundle 2.2.x alphas from https://www.torproject.org/dist/torbrowser/ or run Torbutton in its own separate Firefox profile.

   The reasons for this shift are explained here: https://blog.torproject.org/blog/toggle-or-not-toggle-end-torbutton

   If you find bugs specific to Firefox 5, toggling, and/or extension conflicts, file them under the component "Torbutton": https://trac.torproject.org/projects/tor/report/14

   Bugs that still apply to Tor Browser should be filed under component "TorBrowserButton": https://trac.torproject.org/projects/tor/report/39

   Bugs in the "Torbutton" component currently have no maintainer available to fix them. Feel free to step up.

   Here is the complete changelog:

```
* bug 3101: Disable WebGL. Too many unknowns for now.
* bug 3345: Make Google Captcha redirect work again.
* bug 3399: Fix a reversed exception check found by arno.
* bug 3177: Update torbutton to use new TorBrowser prefs.
* bug 2843: Update proxy preferences window to support env var.
* bug 2338: Force toggle at startup if tor is enabled
* bug 3554: Make Cookie protections obey disk settings
* bug 3441: Enable cookie protection UI by default.
* bug 3446: We're Firefox 5.0, we swear.
```

```
 * bug 3506: Remove window resize event listener.
 * bug 1282: Set fixed window size for each new window.
 * bug 3508: Apply Stanford SafeCache patch (thanks Edward, Collin et
 * al).
 * bug 2361: Make about window work again on FF4+.
 * bug 3436: T(A)ILS was renamed to Tails.
 * bugfix: Fix a transparent context menu issue on Linux FF4+.
 * misc: Squelch exception from app launcher in error console.
 * misc: Make DuckDuckGo the default Google Captcha redirect
 * destination.
 * misc: Make it harder to accidentally toggle torbutton.
```

1. https://www.torproject.org/torbutton/en/design/requirements

2. On July 7th, we released the latest in the 0.2.2x release candidate branch.

   Tor 0.2.2.30-rc is the first release candidate for the Tor 0.2.2.x series. It fixes a few smaller bugs, but generally appears stable. Please test it and let us know whether it is!

```
Changes in version 0.2.2.30-rc - 2011-07-07
  o Minor bugfixes:
    - Send a SUCCEEDED stream event to the controller when a reverse
      resolve succeeded. Fixes bug 3536; bugfix on 0.0.8pre1. Issue
      discovered by katmagic.
    - Always NUL-terminate the sun_path field of a sockaddr_un before
      passing it to the kernel. (Not a security issue: kernels are
      smart enough to reject bad sockaddr_uns.) Found by Coverity;
      CID #428. Bugfix on Tor 0.2.0.3-alpha.
    - Don't stack-allocate the list of supplementary GIDs when we're
      about to log them. Stack-allocating NGROUPS_MAX gid_t elements
      could take up to 256K, which is way too much stack. Found by
      Coverity; CID #450. Bugfix on 0.2.1.7-alpha.
    - Add BUILDTIMEOUT_SET to the list returned by the 'GETINFO
      events/names' control-port command. Bugfix on 0.2.2.9-alpha;
      fixes part of bug 3465.
    - Fix a memory leak when receiving a descriptor for a hidden
      service we didn't ask for. Found by Coverity; CID #30. Bugfix
      on 0.2.2.26-beta.

  o Minor features:
    - Update to the July 1 2011 Maxmind GeoLite Country database.
```

3. On July 17th, we released the latest in the Arm relay controller, 1.4.3. This completes the codebase refactoring project that's been a year in the works and provides numerous performance, usability, and stability improvements...

```
 * Relay Setup Wizard
```

```
Setting up a relay can be tricky for new users. In headless
environments this means navigating Tor's massive, user unfriendly man
page and even when Vidalia's an option it makes relatively poor exit
configurations. Starting arm before Tor now provides instructions for
auto-generating a good relay setup...

  a. Selection for what you'd like to be
      http://www.atagar.com/transfer/tmp/arm_wizard1.png
  b. Picking your relay options
      http://www.atagar.com/transfer/tmp/arm_wizard2.png
  c. Confirmation for the configuration it's making
      http://www.atagar.com/transfer/tmp/arm_wizard3.png

* Menu Interface
All of arm's capabilities are now available via a simple menu interface.
http://www.atagar.com/transfer/tmp/arm_menu.png

* Arm Gui Prototype
Over this summer Kamran Khan has been working on a GTK frontend for
arm as part of Google Summer of Code. The initial prototype is ready!
http://inspirated.com/2011/06/28/summer-of-code-progress-graphs-logs-and-acid

* Performance Improvements
Several arm and TorCtl performance fixes providing a 83% faster
startup time, 12% lower memory usage, and instantaneous shutdown.

* Improved Platform Support
Vastly better support for Mac OSX. Arm has also been backported to
Debian Squeeze and Ubuntu Lucid / Maverick.
http://packages.debian.org/squeeze-backports/tor-arm
https://bugs.launchpad.net/maverick-backports/+bug/721886

* ... etc
Options for requesting a new identity, shutting down Tor, reconnecting
if Tor's been restarted and many, many bugfixes.
http://www.atagar.com/arm/releaseNotes.php#1.4.3
```

4. On July 18th, we released the latest in the experimental branch of Tor 0.2.3.x-alpha.

   Tor 0.2.3.2-alpha introduces two new experimental features: microdescriptors and pluggable transports. It also continues cleaning up a variety of recently introduced features. We are not producing packages for the 0.2.3.x branch until 0.2.2.x is the new -stable. Three sets of packages is beyond our capabilities to create and display right now.

```
Changes in version 0.2.3.2-alpha - 2011-07-18
  o Major features:
```

```
    - Clients can now use microdescriptors instead of regular
      descriptors
      to build circuits. Microdescriptors are authority-generated
      summaries of regular descriptors' contents, designed to change
      very rarely (see proposal 158 for details). This feature is
      designed to save bandwidth, especially for clients on slow
internet
      connections. It's off by default for now, since nearly no caches
      support it, but it will be on-by-default for clients in a future
      version. You can use the UseMicrodescriptors option to turn it on.
    - Tor clients using bridges can now be configured to use a separate
      'transport' proxy for each bridge. This approach helps to resist
      censorship by allowing bridges to use protocol obfuscation
      plugins. It implements part of proposal 180. Implements ticket
2841.
    - While we're trying to bootstrap, record how many TLS connections
      fail in each state, and report which states saw the most failures
      in response to any bootstrap failures. This feature may speed up
      diagnosis of censorship events. Implements ticket 3116.

  o Major bugfixes (on 0.2.3.1-alpha):
    - When configuring a large set of nodes in EntryNodes (as with
      'EntryNodes {cc}' or 'EntryNodes 1.1.1.1/16'), choose only a
      random subset to be guards, and choose them in random
      order. Fixes bug 2798.
    - Tor could crash when remembering a consensus in a non-used
      consensus
      flavor without having a current consensus set. Fixes bug 3361.
    - Comparing an unknown address to a microdescriptor's shortened exit
      policy would always give a "rejected" result. Fixes bug 3599.
    - Using microdescriptors as a client no longer prevents Tor from
      uploading and downloading hidden service descriptors. Fixes
      bug 3601.

  o Minor features:
    - Allow nameservers with IPv6 address. Resolves bug 2574.
    - Accept attempts to include a password authenticator in the
      handshake, as supported by SOCKS5. This handles SOCKS clients that
      don't know how to omit a password when authenticating. Resolves
      bug 1666.
    - When configuring a large set of nodes in EntryNodes, and there are
      enough of them listed as Guard so that we don't need to consider
      the non-guard entries, prefer the ones listed with the Guard flag.
    - Check for and recover from inconsistency in the microdescriptor
      cache. This will make it harder for us to accidentally free a
```

```
    microdescriptor without removing it from the appropriate data
    structures. Fixes issue 3135; issue noted by "wanoskarnet".
  - Log SSL state transitions at log level DEBUG, log domain
    HANDSHAKE. This can be useful for debugging censorship events.
    Implements ticket 3264.
  - Add port 6523 (Gobby) to LongLivedPorts. Patch by intrigeri;
    implements ticket 3439.

o Minor bugfixes (on 0.2.3.1-alpha):
  - Do not free all general-purpose regular descriptors just
    because microdescriptor use is enabled. Fixes bug 3113.
  - Correctly link libevent_openssl when --enable-static-libevent
    is passed to configure. Fixes bug 3118.
  - Bridges should not complain during their heartbeat log messages
    that
    they are unlisted in the consensus: that's more or less the point
    of being a bridge. Fixes bug 3183.
  - Report a SIGNAL event to controllers when acting on a delayed
    SIGNAL NEWNYM command. Previously, we would report a SIGNAL
    event to the controller if we acted on a SIGNAL NEWNYM command
    immediately, and otherwise not report a SIGNAL event for the
    command at all. Fixes bug 3349.
  - Fix a crash when handling the SIGNAL controller command or
    reporting ERR-level status events with bufferevents enabled. Found
    by Robert Ransom. Fixes bug 3367.
  - Always ship the tor-fw-helper manpage in our release tarballs.
    Fixes bug 3389. Reported by Stephen Walker.
  - Fix a class of double-mark-for-close bugs when bufferevents
    are enabled. Fixes bug 3403.
  - Update tor-fw-helper to support libnatpmp-20110618. Fixes bug
    3434.
  - Add SIGNAL to the list returned by the 'GETINFO events/names'
    control-port command. Fixes part of bug 3465.
  - Prevent using negative indices during unit test runs when
    read_all()
    fails. Spotted by coverity.
  - Fix a rare memory leak when checking the nodelist without it being
    present. Found by coverity.
  - Only try to download a microdescriptor-flavored consensus from
    a directory cache that provides them.

o Minor bugfixes (on 0.2.2.x and earlier):
  - Assert that hidden-service-related operations are not performed
    using single-hop circuits. Previously, Tor would assert that
    client-side streams are not attached to single-hop circuits,
```

```
    but not that other sensitive operations on the client and service
    side are not performed using single-hop circuits. Fixes bug 3332;
    bugfix on 0.0.6.
  - Don't publish a new relay descriptor when we reload our onion key,
    unless the onion key has actually changed. Fixes bug 3263 and
    resolves another cause of bug 1810. Bugfix on 0.1.1.11-alpha.
  - Allow GETINFO fingerprint to return a fingerprint even when
    we have not yet built a router descriptor. Fixes bug 3577;
    bugfix on 0.2.0.1-alpha.
  - Make 'tor --digests' list hashes of all Tor source files. Bugfix
    on 0.2.2.4-alpha; fixes bug 3427.

o Code simplification and refactoring:
  - Use tor_sscanf() in place of scanf() in more places through the
    code. This makes us a little more locale-independent, and
    should help shut up code-analysis tools that can't tell
    a safe sscanf string from a dangerous one.
  - Use tt_assert(), not tor_assert(), for checking for test failures.
    This makes the unit tests more able to go on in the event that
    one of them fails.
  - Split connection_about_to_close() into separate functions for each
    connection type.

o Build changes:
  - On Windows, we now define the _WIN32_WINNT macros only if they
    are not already defined. This lets the person building Tor decide,
    if they want, to require a later version of Windows.
```

5. On July 28th, we released an updated Orweb for Android devices. The big news is that you can use this on any Android device without root. Just install Orbot, connect to Tor, then install this, and you are ready to browse like an onion.

   The main issue we are concerned about tracking down is DNS leaks with how we are proxying. We have to use HTTP/S proxy support for now, but it does seem to be resolving names via Tor, since .onion addresses do work. From here, I'll be talking more with mikeperry about all of the possible things we can do to further lockdown webkit, which is the basis for rweb.

   You can grab the direct binary and sig from: https://github.com/guardianproject/Orweb/downloads

   Orweb v2 (0.2.1) - now supports Android 2.x and 3.x

   Use with Orbot on any Android device without any complex configuration. It just works right out of the box.. err, market! Also blocks flash and optionally javascript, and other malicious downloads. Integrates directly with DuckDuckGo.com's search hidden service for private, anonymous searching.

   updated market page: https://market.android.com/details?id=info.guardianproject.browserfeature=search,r

Directly binary download: https://github.com/guardianproject/Orweb/Orwebv2-280711-0.2.1.b.apk/qr*code*

Source and project: https://github.com/guardianproject/Orweb/tree/v0.2.1

Orweb is a privacy enhanced web browser that support proxies. When used with the Orbot (Tor on Android) app, this web browser provides enhanced privacy features. Through Tor, it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked. It also blocks cookies, keeps no local history, disables Flash, and requires only Internet permissions, keeping you safe from malicious content. Finally, beyond Tor, it can support any HTTP proxy server.

```
What's in this version:
- added Android 2.x and 3.x support
- new localization / languages
- integrated DuckDuckGo.com search engine
- new icon!
```

6. On July 13th, all of the alpha Tor Browser Bundles have been updated to the latest Tor 0.2.2.30-rc, and the Windows stable bundle has been updated with the latest Firefox 3.6.19.

   The experimental bundles also now contain Firefox 5 and Polipo has been removed from all of them.

```
Firefox 3.6 Tor Browser Bundles

Windows bundle
1.3.26: Released 2011-07-13

    Update Firefox to 3.6.19
    Update HTTPS-Everywhere to 1.0.0development.4
    Update Libevent to 2.0.12-stable

OS X bundle
1.1.22: Released 2011-07-13

    Update Tor to 0.2.2.30-rc
    Update Firefox to 3.6.19
    Update HTTPS-Everywhere to 1.0.0development.4
    Update NoScript to 2.1.1.2

Linux bundles
1.1.12: Released 2011-07-13

    Update Tor to 0.2.2.30-rc
    Update Firefox to 3.6.19
    Update HTTPS-Everywhere to 1.0.0development.4
    Update NoScript to 2.1.1.2
```

```
Firefox 4 Tor Browser Bundles

Tor Browser Bundle (2.2.30-1)

    Update Tor to 0.2.2.30-rc
    Update Firefox to 5.0.1
    Update Torbutton to 1.4.0
    Update Libevent to 2.0.12-stable
    Update HTTPS-Everywhere to 1.0.0development.4
    Update NoScript to 2.1.1.2
```

Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- The beta censorship detector is deployed. The current BETA version of the censorship detector analyzes the estimated daily user numbers from all countries and from a given country to calculate an estimated range of daily users from that country. Whenever the user number of a country falls outside this range, the censorship detector marks the event either as downturn, which is a possible censorship event, or upturn, which is a potential end of censorship. The BETA version of the algorithm still needs some fine-tuning to reduce the number of false positives." The next step will be to add a tech report or short description about how the detector works. Here's an example graph that contains upturns in blue and downturns in red: `https://metrics.torproject.org/users.html?graph=direct-users&start=2011-01-01&end=2011-08-04&country=ly&events=on&dpi=72#direct-users`

- Started reviewing patches to the bridge database infrastructure. A big change will be supporting reCAPTCHA for bridge address distribution. A challenge is to use reCAPTCHA technology without giving Google all of the IP addresses of users looking for bridges.

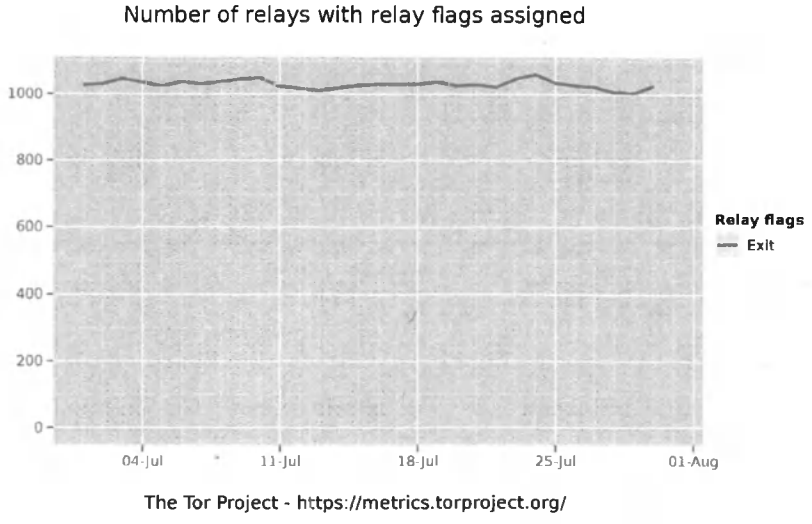
- bridges.torproject.org is accessible via IPv6 directly.

Hide Tor's network signature.

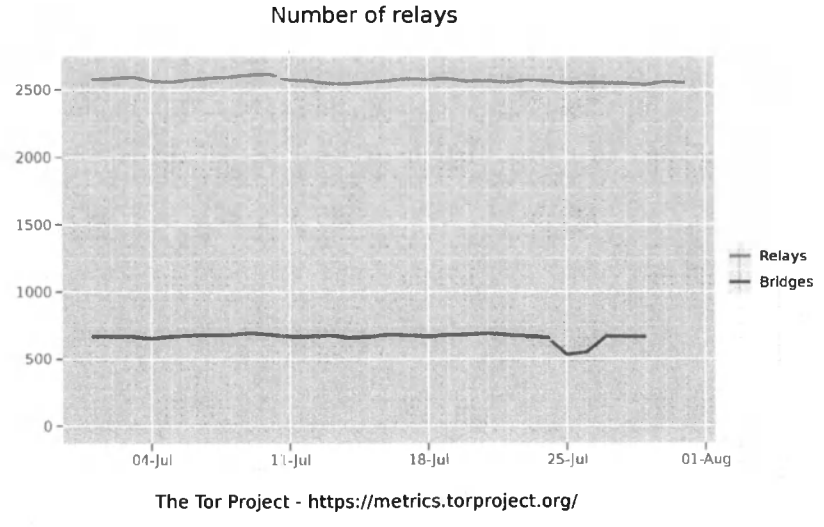
- Progress on obfsproxy continues. It's now more portable, compiling on OS X, linuxes, and MS Windows. Signal handling matches the proposed 180 Pluggable Transport spec, `https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/180-pluggable-transport.txt`. Updated the HOWTO document for users, `https://gitweb.torproject.org/obfsproxy.git/blob/HEAD:/doc/tor-obfs-howto.txt`.

Grow the Tor network and user base. Outreach.

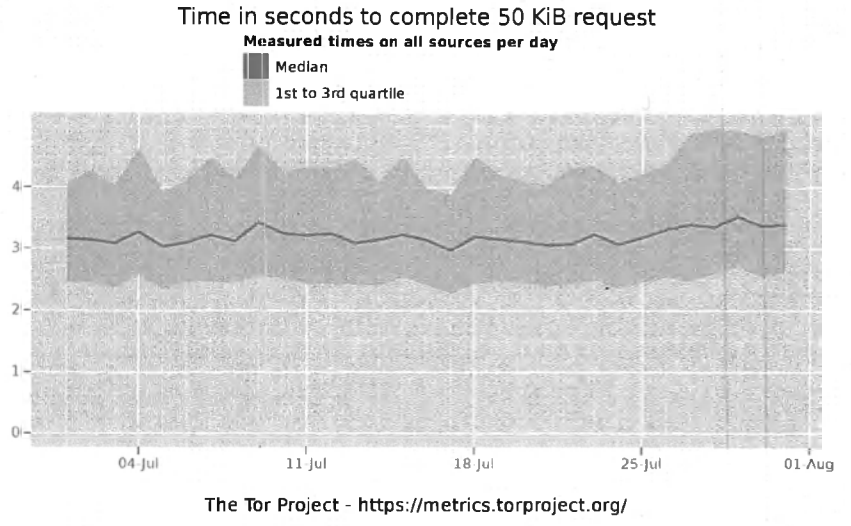
Measures of the Tor Network



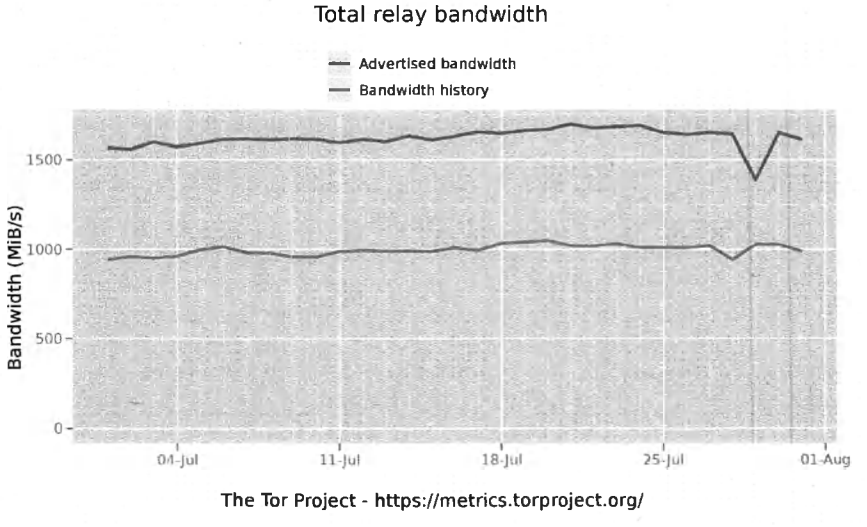
This graph shows the total quantity of exit relays in July 2011. We seem to have kept most of our relays since the bump due to the EFF Tor challenge started in May 2011.



This graph shows the total quantity of relays and the total quantity of bridges in July 2011. We seem to have kept most of our relays since the bump due to the EFF Tor Challenge started in May 2011.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Performance remains relatively steady at just under 4 seconds.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The steady-state of relays creates almost 1.6GBps (12.8 Gbps) of bandwidth available.

Outreach and Advocacy

1. Jacob attended Recon in Montreal.

2. Jacob spoke at something
3. Tor held the annual dev meeting, this year sponsored by the University of Waterloo.
4. Many members of Tor attended the Privacy Enhancing Technology Symposium at the University of Waterloo, `http://petsymposium.org/2011/`.
5. Andrew and Karen spoke to staffers from Senators Casey, Menendez, and Kirk about Internet circumvention and privacy.
6. Andrew and Karen spoke at Radio Liberty's office to a number of press, foundations, and think tanks about Internet censorship and privacy.
7. Andrew and Karen spoke to the Helsinki Commission about Internet censorship and privacy.
8. Runa gave a talk about Tor at the University College of London's School of Oriental and African Studies, `http://www.soas.ac.uk/`.
9. Roger was a panelist on the PETS 'ethics of Tor research' panel.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- See the Tor Browser Bundle updates in the first section. These include new bundles based on Firefox 5.

Bridge relay and bridge authority work.

Started a design for bridges should pick their own guard hop to address some potential risks to clients of bridges.

Scalability, load balancing, directory overhead, efficiency.

- Thanks to an updated Coverity scan, fixed a number of bugs. These are seen in the tor release notes as attributed to Coverity.
- Fixed a number of microdescriptor bugs. Microdescriptors in the master branch are now on-by-default for clients.

Incentives work.

Nothing to report.

More reliable (e.g. split) download mechanism.

Nothing to report.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- Had a conf call with a group of translators in DC who are working on both Arabic and Persian translations of the website. We believe they will finish translating the website by the end of August.
- Fixed a problem with the German .wmi files (3526), included updated docs/de/sidenav.wmi (3538), included a German video on tor-doc-windows.html.de (3532), decided to include the English video as well (3581), included pt_BR translations of two .wmi files (3568), updated Makefile.common to include pt-br when building the website (3579), updated Makefile.common and include/perl-globals.wmi to include more languages when building the website (3625).
- Configured stunnel to work with the transifex-client (3576). This means that we can connect to the Transifex server using HTTPS, while also verifying the certificate.
- Updated translations for German, Arabic, Farsi, Russian, Italian, French, Finnish, Vietnamese, and Chinese.

December 14, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-eighth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at [redacted] if there are any questions.

Invoice 38:

Period	Months	Rate	Cost
05/17/2011 - 06/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG07112011

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: July 13, 2011

This report documents progress in June 2011 on contract BBGCON1807S6441 between BBG and The Tor Project.

New releases, new hires, new funding

New Funding

The US National Science Foundation funds the second year of grant number CNS-0959138. This funds research into Tor Metrics. This grant is the main driver behind `https://metrics.torproject.org`.

New Releases

1. On June 4th we released the latest in the -beta series, Tor 0.2.2.28-beta. Tor 0.2.2.28-beta makes great progress towards a new stable release: we fixed a big bug in whether relays stay in the consensus consistently, we moved closer to handling bridges and hidden services correctly, and we started the process of better handling the dreaded "my Vidalia died, and now my Tor demands a password when I try to reconnect to it" usability issue.

```
Changes in version 0.2.2.28-beta
  o Major bugfixes:
    - Don't decide to make a new descriptor when receiving a HUP signal.
      This bug has caused a lot of 0.2.2.x relays to disappear from the
      consensus periodically. Fixes the most common case of triggering
      bug 1810; bugfix on 0.2.2.7-alpha.
    - Actually allow nameservers with IPv6 addresses. Fixes bug 2574.
    - Don't try to build descriptors if "ORPort auto" is set and we
      don't know our actual ORPort yet. Fix for bug 3216; bugfix on
      0.2.2.26-beta.
    - Resolve a crash that occurred when setting BridgeRelay to 1 with
      accounting enabled. Fixes bug 3228; bugfix on 0.2.2.18-alpha.
    - Apply circuit timeouts to opened hidden-service-related circuits
      based on the correct start time. Previously, we would apply the
      circuit build timeout based on time since the circuit's creation;
      it was supposed to be applied based on time since the circuit
      entered its current state. Bugfix on 0.0.6; fixes part of bug 1297.
```

- Use the same circuit timeout for client-side introduction circuits as for other four-hop circuits, rather than the timeout for single-hop directory-fetch circuits; the shorter timeout may have been appropriate with the static circuit build timeout in 0.2.1.x and earlier, but caused many hidden service access attempts to fail with the adaptive CBT introduced in 0.2.2.2-alpha. Bugfix on 0.2.2.2-alpha; fixes another part of bug 1297.
- In ticket 2511 we fixed a case where you could use an unconfigured bridge if you had configured it as a bridge the last time you ran Tor. Now fix another edge case: if you had configured it as a bridge but then switched to a different bridge via the controller, you would still be willing to use the old one. Bugfix on 0.2.0.1-alpha; fixes bug 3321.

o Major features:
- Add an __OwningControllerProcess configuration option and a TAKEOWNERSHIP control-port command. Now a Tor controller can ensure that when it exits, Tor will shut down. Implements feature 3049.
- If "UseBridges 1" is set and no bridges are configured, Tor will now refuse to build any circuits until some bridges are set. If "UseBridges auto" is set, Tor will use bridges if they are configured and we are not running as a server, but otherwise will make circuits as usual. The new default is "auto". Patch by anonym, so the Tails LiveCD can stop automatically revealing you as a Tor user on startup.

o Minor bugfixes:
- Fix warnings from GCC 4.6's "-Wunused-but-set-variable" option.
- Remove a trailing asterisk from "exit-policy/default" in the output of the control port command "GETINFO info/names". Bugfix on 0.1.2.5-alpha.
- Use a wide type to hold sockets when built for 64-bit Windows builds. Fixes bug 3270.
- Warn when the user configures two HiddenServiceDir lines that point to the same directory. Bugfix on 0.0.6 (the version introducing HiddenServiceDir); fixes bug 3289.
- Remove dead code from rend_cache_lookup_v2_desc_as_dir. Fixes part of bug 2748; bugfix on 0.2.0.10-alpha.
- Log malformed requests for rendezvous descriptors as protocol warnings, not warnings. Also, use a more informative log message in case someone sees it at log level warning without prior info-level messages. Fixes the other part of bug 2748; bugfix on 0.2.0.10-alpha.
- Clear the table recording the time of the last request for each hidden service descriptor from each HS directory on SIGNAL NEWNYM.

```
    Previously, we would clear our HS descriptor cache on SIGNAL
    NEWNYM, but if we had previously retrieved a descriptor (or tried
    to) from every directory responsible for it, we would refuse to
    fetch it again for up to 15 minutes. Bugfix on 0.2.2.25-alpha;
    fixes bug 3309.
  - Fix a log message that said "bits" while displaying a value in
    bytes. Found by wanoskarnet. Fixes bug 3318; bugfix on
    0.2.0.1-alpha.
  - When checking for 1024-bit keys, check for 1024 bits, not 128
    bytes. This allows Tor to correctly discard keys of length 1017
    through 1023. Bugfix on 0.0.9pre5.

o Minor features:
  - Relays now log the reason for publishing a new relay descriptor,
    so we have a better chance of hunting down instances of bug 1810.
    Resolves ticket 3252.
  - Revise most log messages that refer to nodes by nickname to
    instead use the "$key=nickname at address" format. This should be
    more useful, especially since nicknames are less and less likely
    to be unique. Resolves ticket 3045.
  - Log (at info level) when purging pieces of hidden-service-client
    state because of SIGNAL NEWNYM.

o Removed options:
  - Remove undocumented option "-F" from tor-resolve: it hasn't done
    anything since 0.2.1.16-rc.
```

2. On June 20th, we released the latest in the -beta series, Tor 0.2.2.29-beta. Tor 0.2.2.29-beta reverts an accidental behavior change for users who have bridge lines in their torrc but don't want to use them; gets us closer to having the control socket feature working on Debian; and fixes a variety of smaller bugs.

```
Changes in version 0.2.2.29-beta
o Major bugfixes:
  - Revert the UseBridges option to its behavior before 0.2.2.28-beta.
    When we changed the default behavior to "use bridges if any
    are listed in the torrc", we surprised users who had bridges
    in their torrc files but who didn't actually want to use them.
    Partial resolution for bug 3354.

o Privacy fixes:
  - Don't attach new streams to old rendezvous circuits after SIGNAL
    NEWNYM. Previously, we would keep using an existing rendezvous
    circuit if it remained open (i.e. if it were kept open by a
    long-lived stream, or if a new stream were attached to it before
```

```
    Tor could notice that it was old and no longer in use). Bugfix on
    0.1.1.15-rc; fixes bug 3375.

  o Minor bugfixes:
    - Fix a bug when using ControlSocketsGroupWritable with User. The
      directory's group would be checked against the current group, not
      the configured group. Patch by Jérémy Bobbio. Fixes bug 3393;
      bugfix on 0.2.2.26-beta.
    - Make connection_printf_to_buf()'s behaviour sane. Its callers
      expect it to emit a CRLF iff the format string ends with CRLF;
      it actually emitted a CRLF iff (a) the format string ended with
      CRLF or (b) the resulting string was over 1023 characters long or
      (c) the format string did not end with CRLF *and* the resulting
      string was 1021 characters long or longer. Bugfix on 0.1.1.9-alpha;
      fixes part of bug 3407.
    - Make send_control_event_impl()'s behaviour sane. Its callers
      expect it to always emit a CRLF at the end of the string; it
      might have emitted extra control characters as well. Bugfix on
      0.1.1.9-alpha; fixes another part of bug 3407.
    - Make crypto_rand_int() check the value of its input correctly.
      Previously, it accepted values up to UINT_MAX, but could return a
      negative number if given a value above INT_MAX+1. Found by George
      Kadianakis. Fixes bug 3306; bugfix on 0.2.2pre14.
    - Avoid a segfault when reading a malformed circuit build state
      with more than INT_MAX entries. Found by wanoskarnet. Bugfix on
      0.2.2.4-alpha.
    - When asked about a DNS record type we don't support via a
      client DNSPort, reply with NOTIMPL rather than an empty
      reply. Patch by intrigeri. Fixes bug 3369; bugfix on 2.0.1-alpha.
    - Fix a rare memory leak during stats writing. Found by coverity.

  o Minor features:
    - Update to the June 1 2011 Maxmind GeoLite Country database.

  o Code simplifications and refactoring:
    - Remove some dead code as indicated by coverity.
    - Remove a few dead assignments during router parsing. Found by
      coverity.
    - Add some forgotten return value checks during unit tests. Found
      by coverity.
    - Don't use 1-bit wide signed bit fields. Found by coverity.
```

3. On June 12th, the anonymous operating system, Tails, version 0.7.2 was released. This release fixes some critical bugs in the included software.

```
   * Iceweasel
```

```
- Disable Torbutton's external application launch warning.
  ... which advises using Tails. Tails *is* running Tails.
- FoxyProxy: install from Debian instead of the older one we previously
  shipped.

* Software
- haveged: install an official Debian backport instead of a custom backport.
- unrar: install the version from Debian's non-free repository.
  Users report unrar-free does not work well enough.
```

4. On June 25th, we released new Tor Browser Bundles. All of the alpha Tor Browser Bundles have been updated to the latest Tor 0.2.2.29-beta.

   Firefox 5 has recently been released and our next set of Firefox alpha bundles will come with that instead of Firefox 4. For users who want to use Firefox 5 now, Torbutton 1.3.3-alpha is compatible.

   We're also going to begin phasing out the Firefox 3.6 bundles within the next month. Mike Perry is focusing his attention on the new Firefox releases and we feel this is the best path to keep our users safe. You can also see his current Firefox patches in the Tor Browser Bundle git repository.

   The following changelogs encompass the would-be Tor 0.2.2.28-beta packages as well as the changes made for Tor 0.2.2.29-beta.

```
Firefox 3.6 Tor Browser Bundles

OS X bundle
1.1.19: Released 2011-06-21

    * Update Tor to 0.2.2.29-beta
    * Update NoScript to 2.1.1.1
    * Update HTTPS-Everywhere to 0.9.9.development.6

1.0.18: Released 2011-06-05

    * Update Tor to 0.2.2.28-beta
    * Update Libevent to 2.0.12-stable
    * Update zlib to 1.2.5
    * Update NoScript to 2.1.1
    * Update BetterPrivacy to 1.51

Linux bundles
1.1.11: Released 2011-06-21

    * Update Tor to 0.2.2.29-beta
    * Update NoScript to 2.1.1.1
```

```
    * Update HTTPS-Everywhere to 0.9.9.development.6

1.1.10: Released 2011-06-05

    * Update Tor to 0.2.2.28-beta
    * Update Libevent to 2.0.12-stable
    * Update zlib to 1.2.5
    * Update NoScript to 2.1.1
    * Update BetterPrivacy to 1.51

Firefox 4 Tor Browser Bundles

Tor Browser Bundle (2.2.29-1)

    * Update Tor to 0.2.2.29-beta
    * Update Libevent to 2.0.12-stable
    * Update HTTPS Everywhere to 0.9.9.development.6
    * Update NoScript to 2.1.1.1
    * Update BetterPrivacy to 1.51
```

5. On June 4th, released the latest in the libevent -stable series, 2.0.12.

```
BUGFIXES
 o Fix a warn-and-fail bug in kqueue by providing kevent() room to report
 errors (28317a0)
 o Fix an assert-inducing fencepost bug in the select backend (d90149d)
 o Fix failing http assertion introducd in commit 0d6622e (0848814 .
 Kevin Ko)
 o Fix a bug that prevented us from configuring IPv6 nameservers. (74760f1)
 o Prevent size_t overflow in evhttp_htmlescape. (06c51cd Mansour Moufid)
 o Added several checks for under/overflow conditions in
 evhttp_handle_chunked_read (a279272 Mark Ellzey)
 o Added overflow checks in evhttp_read_body and evhttp_get_body (84560fc
 Mark Ellzey)

DOCUMENTATION:
 o Add missing words to EVLOOP_NONBLOCK documentation (9556a7d)

BUILD FIXES
 o libssl depends on libcrypto, not the other way around. (274dd03
 Peter Rosin)
 o Libtool brings in the dependencies of libevent_openssl.la automatically
 (7b819f2 Peter Rosin)
 o Use OPENSSL_LIBS in Makefile.am (292092e Sebastian Hahn)
 o Move the win32 detection in configure.in (ceb03b9 Sebastian Hahn)
```

o Correctly detect openssl on windows (6619385 Sebastian Hahn)
o Fix a compile warning with zlib 1.2.4 and 1.2.5 (5786b91 Sebastian Hahn)
o Fix compilation with GCC 2, which had no __builtin_expect (09d39a1 Dave Hart)
o Fix new warnings from GCC 4.6 (06a714f)
o Link with -lshell32 and -ladvapi32 on Win32. (86090ee Peter Rosin)
o Make the tests build when OpenSSL is not available. (07c41be Peter Rosin)
o Bring in the compile script from automake, if needed. (f3c7a4c Peter Rosin)
o MSVC does not provide S_ISDIR, so provide it manually. (70be7d1 Peter Rosin)
o unistd.h and sys/time.h might not exist. (fe93022 Peter Rosin)
o Make sure TINYTEST_LOCAL is defined when building tinytest.c (8fa030c Peter Rosin)
o Fix winsock2.h #include issues with MSVC (3d768dc Peter Rosin)
o Use evutil_gettimeofday instead of relying on the system gettimeofday. (0de87fe Peter Rosin)
o Always use evutil_snprintf, even if OS provides it (d1b2d11 Sebastian Hahn)
o InitializeCriticalSectionAndSpinCount requires _WIN32_WINNT >= 0x0403. (816115a Peter Rosin)
o cygwin: make it possible to build DLLs (d54d3fc)

6. On June 30th, we released the latest stable version of torbutton, 1.4.0.

The addon has been disabled on addons.mozilla.org. Our URL is now canonical.

This release features support for Firefox 5.0, and has been tested against the vanilla release for basic functionality. However, it has not been audited for Network Isolation, State Separation, Tor Undiscoverability or Interoperability issues[1] due to toggling under Firefox 5.

If you desire Torbutton functionality with Firefox 4/5, we recommend you download the Tor Browser Bundle 2.2.x alphas from https://www.torproject.org/dist/torbrowser/ or run Torbutton in its own separate Firefox profile.

The reasons for this shift are explained here:
https://blog.torproject.org/blog/toggle-or-not-toggle-end-torbutton

If you find bugs specific to Firefox 5, toggling, and/or extension

```
conflicts, file them under the component "Torbutton":
https://trac.torproject.org/projects/tor/report/14

Bugs that still apply to Tor Browser should be filed under component
"TorBrowserButton":
https://trac.torproject.org/projects/tor/report/39

Bugs in the "Torbutton" component currently have no maintainer
available to fix them. Feel free to step up.

Here is the complete changelog:
* bug 3101: Disable WebGL. Too many unknowns for now.
* bug 3345: Make Google Captcha redirect work again.
* bug 3399: Fix a reversed exception check found by arno.
* bug 3177: Update torbutton to use new TorBrowser prefs.
* bug 2843: Update proxy preferences window to support env var.
* bug 2338: Force toggle at startup if tor is enabled
* bug 3554: Make Cookie protections obey disk settings
* bug 3441: Enable cookie protection UI by default.
* bug 3446: We're Firefox 5.0, we swear.
* bug 3506: Remove window resize event listener.
* bug 1282: Set fixed window size for each new window.
* bug 3508: Apply Stanford SafeCache patch (thanks Edward, Collin et al).
* bug 2361: Make about window work again on FF4+.
* bug 3436: T(A)ILS was renamed to Tails.
* bugfix: Fix a transparent context menu issue on Linux FF4+.
* misc: Squelch exception from app launcher in error console.
* misc: Make DuckDuckGo the default Google Captcha redirect destination.
* misc: Make it harder to accidentally toggle torbutton.

1. https://www.torproject.org/torbutton/en/design/#requirements
```

7. We released two new updates to tordnsel to address a number of bugs and add new features.

```
version 0.1.1 - 2011-06-28
  - Correctly label the release version and Changelog.
  - Add updated website and maintainers in tordnsel.cabal.
  - Document the tordnsel init script for Debian.

version 0.1.0 - 2011-06-28
  o Deployment:
    - Add support for logging messages to stdout, stderr, syslog, or to a file.
      Syslog logging should be useful for running in a chroot.
    - Display better error messages for config file parsing, directory parsing,
      Tor controller errors, I/O errors, and almost every error condition.
    - Add a man page fully documenting config options, signals, files, sockets,
```

and exit codes.
  - Add support for reloading the configuration by reloading the config file when we receive SIGHUP, or by listening for the contents of the config file on a Unix domain socket. The latter is useful for running in a chroot, where the process can't access its own config file.
  - Implement the reload command in the sample init.d script using the new --reconfigure command-line option, which reloads the config file through a Unix domain socket for chroot-friendliness.
  - Exit gracefully when we receive SIGINT or SIGTERM.
  - Add a --verify-config command-line option for checking whether the config file is well-formed without starting TorDNSEL. Apply it in the sample init.d script.
  - Add --help and --version command-line options.

o Reliability:
  - Implement Erlang-style thread links and monitors for error handling.
  - Refactor every thread to support a start/reconfigure/terminate API.
  - Each thread now runs in a fault-tolerant supervision hierarchy in which the thread is responsible for handling errors in its children, and its supervisor handles errors in it. If a thread dies unexpectedly, the reason it died is logged and its supervisor attempts to restart it when possible.

o New required options:
  - Create a new required RuntimeDirectory option for the statistics and reconfigure sockets.
  - Rename the AuthoritativeZone option to ZoneOfAuthority, since name servers are authoritative, not zones.

o Performance:
  - Share copies of exit policy rules and exit policies with a hash table of weak pointers. According to nickm, only 5% of them are distinct.
  - Squash some space leaks in network state updates.

o Standards conformance:
  - Stop requiring that reserved bits in the DNS header be 0.

o Active tests:
  - Replace the ConcurrentExitTests option with EnableActiveTesting, since we now automatically detect limits imposed on open file descriptors by FD_SETSIZE and resource limits.
  - Refactor the exit test initiator to keep a history of scheduled exit tests and dynamically adjust the rate at which tests are initiated. This should smooth out the pubkey crypto demands on Tor that were maxing out CPU utilization.
  - Make a better effort to avoid redundant testing by storing pending tests

```
    in a distinct queue.
  - Stop testing every node periodically between descriptor publications.
    Instead, every hour attempt to test through any exit nodes that haven't
    been successfully tested since they last published a descriptor. This
    should have a similar effect of catching nodes that slipped through an
    earlier attempted test.
  - Regenerate the exit-addresses store every time a new network status
    consensus is received instead of every 15 minutes.
  - Reduce the maximum relay age from 48 hours to 24 hours.  This should
    cut down the length of time a relay is listed in the exitlist after
    it has been disabled or changed to a non-exit relay.

o Controller:
  - Close controller connections cleanly with the QUIT command.
  - Add support for authenticating with PROTOCOLINFO.
  - Set the new FetchDirInfoEarly option to enable fetching dir info on the
    mirror schedule, preferably from authorities.
  - Ensure that config options we set are rolled back to their previous state
    when a controller connection is closed cleanly.
```

Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- Vidalia improvements:

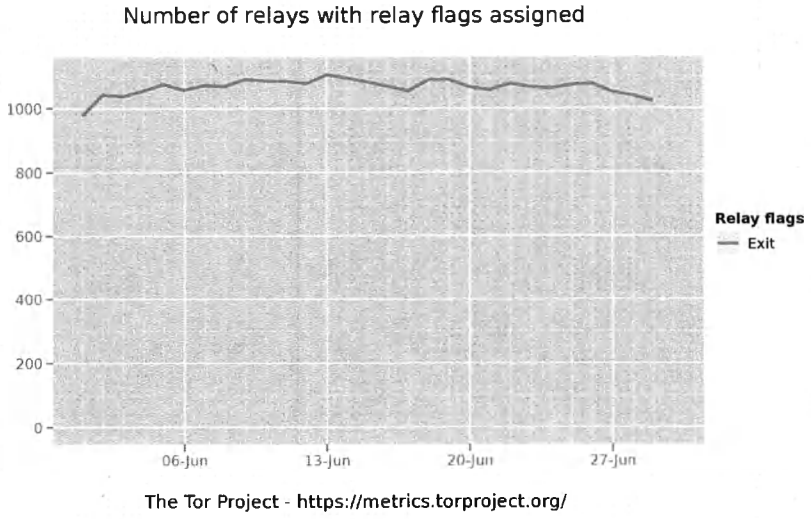
```
Regarding Vidalia:
- worked in the plugin framework. This involved writing the spec,
  working on the engine itself, and then building the interfaces to Qt
  and Vidalia/TorControl. I used qtscriptgenerator to interface Qt,
  which worked really nice and almost out of the box.
- spent a while discussing the problem of the tri-state UseBridges
  feature and preparing a 0.2.13 emergency release, but it never got
  through, and the fixes for this particular case are on stall for now.
- implemented detachable tabs to give more flexibility to plugins, and
  the basice GUI.
- implemented the Vidalia side of the *Port auto feature.

Regarding Vidalia Plugins:
- created a test plugin to implement a testing GUI to
  obfsproxy.
- migrated the TBB code to a plugin, and removed those parts from
  Vidalia.

Regarding Thandy:
- spent some time getting to know the code and discussing different
```

```
    parts of the thp spec with Nick, Robert, and Sebastian.
  - implemented the thp spec, we are about to start testing it with real
    packages. The idea (or at least my idea) is to release this with
    Vidalia-0.3.1, along with the corresponding plugin to control it.
```

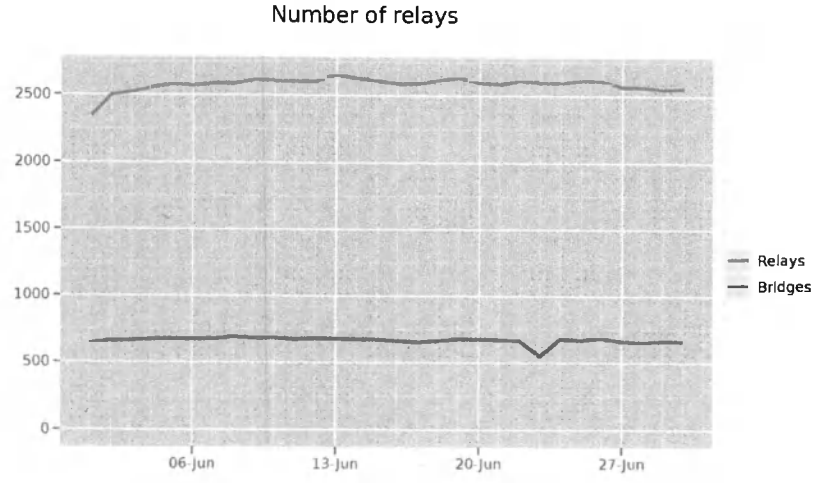
Hide Tor's network signature.

Grow the Tor network and user base. Outreach.

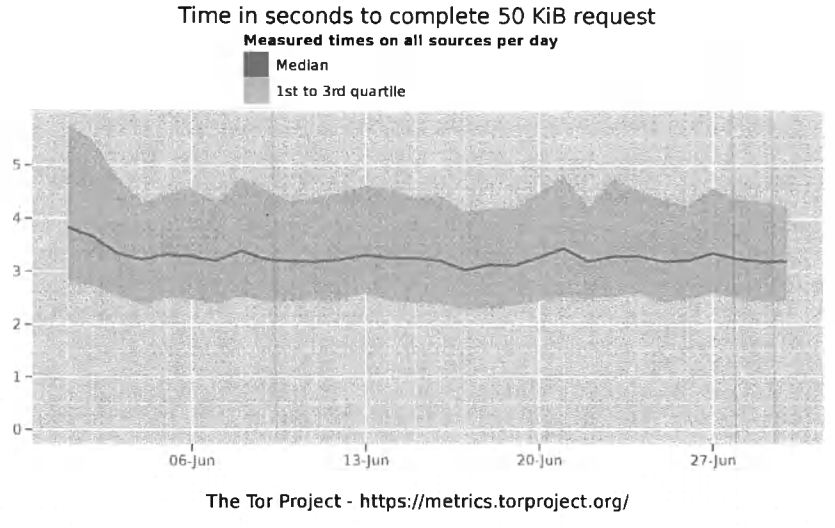
Measures of the Tor Network



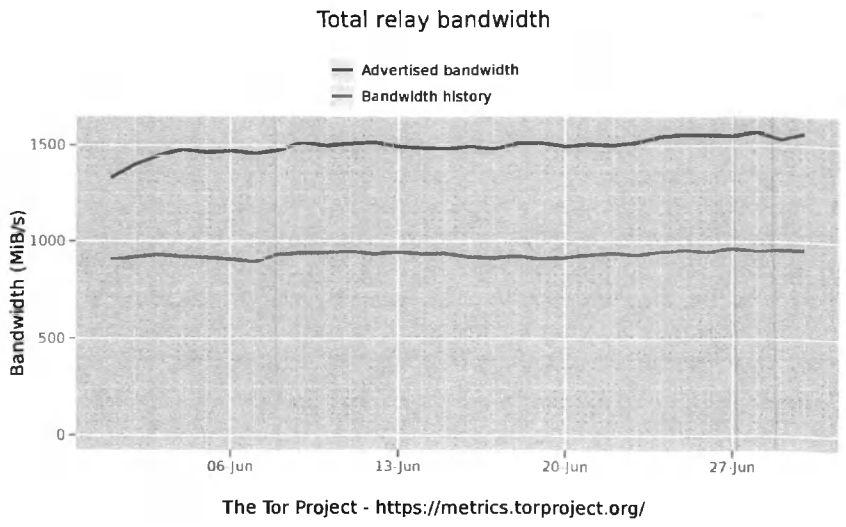
This graph shows the total quantity of exit relays in June 2011. We seem to have kept most of our relays since the bump due to the EFF Tor challenge started in May 2011.



This graph shows the total quantity of relays and the total quantity of bridges in June 2011. We seem to have kept most of our relays since the bump due to the EFF Tor Challenge started in May 2011.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Performance remains relatively steady at just under 4 seconds.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The steady-state of relays creates almost 1.5GBps (12.0 Gbps) of bandwidth available.

Outreach and Advocacy

1. Runa attended the London CyberSecurity Summit, `http://www.cybersummit2011.com/`.
2. Jacob and Linus spoke at the NORDUnet conference, `https://portal.nordu.net/display/ndn2011web/index`.
3. Andrew spoke at the Allied Media conference, `http://alliedmedia.org/`.
4. Jacob spoke at FISL12 in Porto Allegre, Brazil, `http://softwarelivre.org/fisl12`.
5. Tor was featured by CNN for protecting whistleblower's anonymity, `http://www.cnn.com/2011/TECH/web/06/11/hiding.online.identity/index.html`.
6. Tor was featured by CNN for its role in the Arab Spring, `http://www.cnn.com/2011/TECH/innovation/06/17/mesh.technology.revolution/index.html`.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- Mike wrote up his thoughts on improving private browsing modes, `https://blog.torproject.org/blog/improving-private-browsing-modes-do-not-track-vs-real-privacy-design`.
- See the new bundles as released in the "New Releases" section.
- ARM is making tremendous progress over the past month.

Several new features and is now tantalizingly
close to its 1.4.3 release. Improvements include...
* Menu interface (thanks to Kamran for implementing its first version)
* TorCtl fixes for 2412, 2812, 2065, 1329, 2580, 3406, and 3409 [1-7]
* Newnym option
* Dependency auto-fetching via mirrors with signature checks (issue
spotted by Sebastian and Robert)
* Relay setup wizard. This is still in the works and about a week away
from completion, but it's turning out very nicely.

Kamran has made some progress with the arm gui, porting the bandwidth
graphs and nearly finishing the log panel. This has slipped quite a
bit due to illness and family issues, though the parts that are done
look great. For a description and screenshot of his work see his blog
posting [8].

Finally, dug into arm's resource consumption and performance. Reduced its
memory usage by 12% and the shutdown time's now instantaneous. However,
besides this arm's about as lean as one can reasonably make it...

17.9 MB total memory usage
3.0 MB (16.8%) is from the idle python interpretor
7.5 MB (41.9%) is from importing the codebase
7.4 MB (41.3%) is consumed at runtime, contribution from individual
panels being negligible

Startup time is 0.142 seconds. 0.103 is the baseline startup, with
graphing contributing an extra 0.02 seconds (probably from reading the
state file for bandwidth prepopulation). On the first startup there's
around an extra second, probably for importing the libraries.

As for cpu usage, there's spikes from connection and resource usage
fetches but otherwise it's flat (very little curses or controller
activity due to caching and being smart with redraws). Individual
panels don't contribute noticeably to the baseline.

[1] https://trac.torproject.org/projects/tor/ticket/2412
[2] https://trac.torproject.org/projects/tor/ticket/2812
[3] https://trac.torproject.org/projects/tor/ticket/2065
[4] https://trac.torproject.org/projects/tor/ticket/1329
[5] https://trac.torproject.org/projects/tor/ticket/2580
[6] https://trac.torproject.org/projects/tor/ticket/3406
[7] https://trac.torproject.org/projects/tor/ticket/3409
[8] http://inspirated.com/2011/06/28/summer-of-code-progress-graphs-logs-and-acid

Bridge relay and bridge authority work.

Nothing to report.

Scalability, load balancing, directory overhead, efficiency.

- Worked on code to work on the more compact geoip format of bug2506.
- Finished up the implementation for "FooPort auto", which allows Tor to pick which port to use for a given listener.
- Wrote some code for feature3116, which notes where TLS connections are when they fail so that we can more easily diagnose censorship. Still needs merge and review.
- tweaked Robert Hogan's bug1666 branch to receive and handle socks authentication. Still needs merge and review.
- Received and reviewed a patch to enable Tor to work over IPv6. Patch needs work, but progress is being made.
- Got a start on proposal 171 (stream isolation). `https://gitweb.torproject.org/torspec.git/blob/master:/proposals/171-separate-streams.txt`.
- Spent a little while working on agl's curve25519-donna.c implementation, and shaved about 10-25% off its run time.
- Fixed a number of bugs in the torflow codebase related to Bandwidth Authorities. This results in less memory utilization and a few fixes for measurement accuracy. Tickets `https://trac.torproject.org/projects/tor/ticket/1976`, `https://trac.torproject.org/projects/tor/ticket/2391`, and `https://trac.torproject.org/projects/tor/ticket/2861`.

Incentives work.

Nothing to report.

More reliable (e.g. split) download mechanism.

```
Regarding Thandy:
- spent some time getting to know the code and discussing different
  parts of the thp spec with Nick, Robert, and Sebastian.
- implemented the thp spec, we are about to start testing it with real
  packages. The idea (or at least my idea) is to release this with
  Vidalia-0.3.1, along with the corresponding plugin to control it.
```

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- Updated translations in Arabic, German, French, Spanish, Farsi, Russian, Italian, and Polish.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: April 8, 2011

This report documents progress in March 2011 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

New Hires

Contracted Tomas Touceda to fix bugs and develop new features for the Tor graphical controller, Vidalia.

New Funding

Tor receives an anonymous donation to improve hidden services performance, reliability, and general bug fixes.

New Releases

1. On March 9th we released updated Tor Browser Bundles for Microsoft Windows, Apple OS X, and GNU/Linux operating systems. All of the Tor Browser Bundles have been updated with Firefox 3.6.15 and the alpha bundles for Mac OS X and Linux have also been updated with Tor 0.2.2.23-alpha.

```
Windows bundles 1.3.20: Released 2011-03-07
Update Firefox to 3.6.15

Linux bundles 1.1.5: Released 2011-03-09
Update Tor to 0.2.2.23-alpha
Update Firefox to 3.6.15
Update NoScript to 2.0.9.8
Update HTTPS-Everywhere to 0.9.9.development.3

OS X bundle 1.0.13: Released 2011-03-09
Update Tor to 0.2.2.23-alpha
Update Firefox to 3.6.15, and use the Mozilla version until I get it to build on OS X 10.6 (Snow L
Update NoScript to 2.0.9.8
Update HTTPS-Everywhere to 0.9.9.development.3
```

2. On March 8th, we released the latest in the tor -alpha series, 0.2.2.23. Tor 0.2.2.23-alpha lets relays record their bandwidth history so when they restart they don't lose their bandwidth

capacity estimate. This release also fixes a diverse set of user-facing bugs, ranging from relays overrunning their rate limiting to clients falsely warning about clock skew to bridge descriptor leaks by our bridge directory authority.

```
Changes in version 0.2.2.23-alpha - 2011-03-08

  o Major bugfixes:
    - Stop sending a CLOCK_SKEW controller status event whenever
      we fetch directory information from a relay that has a wrong clock.
      Instead, only inform the controller when it's a trusted authority
      that claims our clock is wrong. Bugfix on 0.1.2.6-alpha; fixes
      the rest of bug 1074.
    - Fix an assert in parsing router descriptors containing IPv6
      addresses. This one took down the directory authorities when
      somebody tried some experimental code. Bugfix on 0.2.1.3-alpha.
    - Make the bridge directory authority refuse to answer directory
      requests for "all" descriptors. It used to include bridge
      descriptors in its answer, which was a major information leak.
      Found by "piebeer". Bugfix on 0.2.0.3-alpha.
    - If relays set RelayBandwidthBurst but not RelayBandwidthRate,
      Tor would ignore their RelayBandwidthBurst setting,
      potentially using more bandwidth than expected. Bugfix on
      0.2.0.1-alpha. Reported by Paul Wouters. Fixes bug 2470.
    - Ignore and warn if the user mistakenly sets "PublishServerDescriptor
      hidserv" in her torrc. The 'hidserv' argument never controlled
      publication of hidden service descriptors. Bugfix on 0.2.0.1-alpha.

  o Major features:
    - Relays now save observed peak bandwidth throughput rates to their
      state file (along with total usage, which was already saved)
      so that they can determine their correct estimated bandwidth on
      restart. Resolves bug 1863, where Tor relays would reset their
      estimated bandwidth to 0 after restarting.
    - Directory authorities now take changes in router IP address and
      ORPort into account when determining router stability. Previously,
      if a router changed its IP or ORPort, the authorities would not
      treat it as having any downtime for the purposes of stability
      calculation, whereas clients would experience downtime since the
      change could take a while to propagate to them. Resolves issue 1035.
    - Enable Address Space Layout Randomization (ASLR) and Data Execution
      Prevention (DEP) by default on Windows to make it harder for
      attackers to exploit vulnerabilities. Patch from John Brooks.

  o Minor bugfixes (on 0.2.1.x and earlier):
    - Fix a rare crash bug that could occur when a client was configured
      with a large number of bridges. Fixes bug 2629; bugfix on
      0.2.1.2-alpha. Bugfix by trac user "shitlei".
    - Avoid a double mark-for-free warning when failing to attach a
      transparent proxy connection. Bugfix on 0.1.2.1-alpha. Fixes
      bug 2279.
    - Correctly detect failure to allocate an OpenSSL BIO. Fixes bug 2378;
```

found by "cypherpunks". This bug was introduced before the first Tor release, in svn commit r110.
- Country codes aren't supported in EntryNodes until 0.2.3.x, so don't mention them in the manpage. Fixes bug 2450; issue spotted by keb and G-Lo.
- Fix a bug in bandwidth history state parsing that could have been triggered if a future version of Tor ever changed the timing granularity at which bandwidth history is measured. Bugfix on Tor 0.1.1.11-alpha.
- When a relay decides that its DNS is too broken for it to serve as an exit server, it advertised itself as a non-exit, but continued to act as an exit. This could create accidental partitioning opportunities for users. Instead, if a relay is going to advertise reject *:* as its exit policy, it should really act with exit policy "reject *:*". Fixes bug 2366. Bugfix on Tor 0.1.2.5-alpha. Bugfix by user "postman" on trac.
- In the special case where you configure a public exit relay as your bridge, Tor would be willing to use that exit relay as the last hop in your circuit as well. Now we fail that circuit instead. Bugfix on 0.2.0.12-alpha. Fixes bug 2403. Reported by "piebeer".
- Fix a bug with our locking implementation on Windows that couldn't correctly detect when a file was already locked. Fixes bug 2504, bugfix on 0.2.1.6-alpha.
- Fix IPv6-related connect() failures on some platforms (BSD, OS X). Bugfix on 0.2.0.3-alpha; fixes first part of bug 2660. Patch by "piebeer".
- Set target port in get_interface_address6() correctly. Bugfix on 0.1.1.4-alpha and 0.2.0.3-alpha; fixes second part of bug 2660.
- Directory authorities are now more robust to hops back in time when calculating router stability. Previously, if a run of uptime or downtime appeared to be negative, the calculation could give incorrect results. Bugfix on 0.2.0.6-alpha; noticed when fixing bug 1035.
- Fix an assert that got triggered when using the TestingTorNetwork configuration option and then issuing a GETINFO config-text control command. Fixes bug 2250; bugfix on 0.2.1.2-alpha.

o Minor bugfixes (on 0.2.2.x):
- Clients should not weight BadExit nodes as Exits in their node selection. Similarly, directory authorities should not count BadExit bandwidth as Exit bandwidth when computing bandwidth-weights. Bugfix on 0.2.2.10-alpha; fixes bug 2203.
- Correctly clear our dir_read/dir_write history when there is an error parsing any bw history value from the state file. Bugfix on Tor 0.2.2.15-alpha.
- Resolve a bug in verifying signatures of directory objects with digests longer than SHA1. Bugfix on 0.2.2.20-alpha. Fixes bug 2409. Found by "piebeer".
- Bridge authorities no longer crash on SIGHUP when they try to publish their relay descriptor to themselves. Fixes bug 2572. Bugfix on 0.2.2.22-alpha.

```
  o Minor features:
    - Log less aggressively about circuit timeout changes, and improve
      some other circuit timeout messages. Resolves bug 2004.
    - Log a little more clearly about the times at which we're no longer
      accepting new connections. Resolves bug 2181.
    - Reject attempts at the client side to open connections to private
      IP addresses (like 127.0.0.1, 10.0.0.1, and so on) with
      a randomly chosen exit node. Attempts to do so are always
      ill-defined, generally prevented by exit policies, and usually
      in error. This will also help to detect loops in transparent
      proxy configurations. You can disable this feature by setting
      "ClientRejectInternalAddresses 0" in your torrc.
    - Always treat failure to allocate an RSA key as an unrecoverable
      allocation error.
    - Update to the March 1 2011 Maxmind GeoLite Country database.

  o Minor features (log subsystem):
    - Add documentation for configuring logging at different severities in
      different log domains. We've had this feature since 0.2.1.1-alpha,
      but for some reason it never made it into the manpage. Fixes
      bug 2215.
    - Make it simpler to specify "All log domains except for A and B".
      Previously you needed to say "[*,~A,~B]". Now you can just say
      "[~A,~B]".
    - Add a "LogMessageDomains 1" option to include the domains of log
      messages along with the messages. Without this, there's no way
      to use log domains without reading the source or doing a lot
      of guessing.

  o Packaging changes:
    - Stop shipping the Tor specs files and development proposal documents
      in the tarball. They are now in a separate git repository at
      git://git.torproject.org/torspec.git
```

3. On March 24th, all of the Tor Browser Bundles have been updated with Firefox 3.6.16 and the alpha bundles for Mac OS X and Linux have also been updated to use Libevent 2, as well as a number of extension updates. The changelogs are below.

```
Windows bundles 1.3.21: Released 2011-03-23
Update Firefox to 3.6.16
Update HTTPS-Everywhere to 0.9.9.development.4

Linux bundles 1.1.6: Released 2011-03-23
Update Firefox to 3.6.16
Update Libevent to 2.0.10-stable
Update NoScript to 2.0.9.9
Update HTTPS-Everywhere to 0.9.9.development.4
Update BetterPrivacy to 1.49

OS X bundle 1.0.14: Released 2011-03-23
```

```
Update Firefox to 3.6.16
Update Libevent to 2.0.10-stable
Update NoScript to 2.0.9.9
Update HTTPS-Everywhere to 0.9.9.development.4
Update BetterPrivacy to 1.49
```

4. On March 27th, we have new Firefox 4 Tor Browser Bundles available for OS X. They come in 64- and 32-bit versions, and one important fix for 10.6 64-bit users is that Firefox no longer crashes on initial startup. These are alpha, but they are going to be a permanent addition to the Tor Browser Bundle family and will be maintained from now on. These have thus far only been tested on Snow Leopard, but the 32-bit bundle ought to work on Leopard.

```
Tor Browser Bundle (2.2.23-1) alpha; suite=osx
Create new bundles for Firefox 4, both i386 and x86_64 (closes: #2140)
Update Tor to 0.2.2.23-alpha
Update Torbutton to 1.3.2-alpha
Update OpenSSL to 1.0.0d
Update HTTPS-Everywhere to 0.9.9.development.4
Update NoScript to 2.0.9.9
Update BetterPrivacy to 1.49
```

5. On March 31st, we released bridge by default bundles. These were previously released as a technology preview but we're going to bring them back on a consistent basis. We have an updated bridge by default Vidalia bundle for Windows available with Tor 0.2.2.23-alpha.

6. On March 31st, we now have Firefox 4 bundles available for GNU/Linux.

```
Tor Browser Bundle (2.2.23-1) alpha; suite=linux
Create new bundles for Firefox 4, both i386 and x86_64
Update Tor to 0.2.2.23-alpha
Update Torbutton to 1.3.2-alpha
Update OpenSSL to 1.0.0d
Update HTTPS-Everywhere to 0.9.9.development.4
Update NoScript to 2.0.9.9
Update BetterPrivacy to 1.49
```

7. On March 21st, we released the latest in the torbutton alpha branch, version 1.3.2. It fixes a few outstanding bugs and better supports Firefox 4.

```
 * bug 1624: Use nsIDOMCrypto::logout() instead of the SSLv2 pref hack
 * bug 1999: Disable tor:// urls by default
 * bug 1968: Reset window.name on tor toggle
 * bug 2148: Make refspoofing more uniform
 * bug 2359: Fix XHTML DTD errors on FF4
 * bugs 2465+2421: Fix javascript hook exceptions+issues in FF4.0
 * bug 2458: Opt out of Firefox addon usage pings
 * bug 2377: Limit the Google captcha cookies copied between google TLDs
 * bug 2491: Clean up checks for when to jar protected cookies
 * bug 1110: Add popup to ask if we should spoof English Accept: headers
 * misc: Remove a noisy FF2 nsICookieManager2 fallback check.
```

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

1. Jacob did research into and wrote up his analysis of suspicious SSL certificates from Comodo, https://blog.torproject.org/blog/detecting-certificate-authority-compromises-and-web-brow
2. Mike wrote a client for EFF's SSL Observatory to provide users with the ability to opt-in to submitting "strange" SSL certificates.
3. Mike helped write a paper for the W3C Workshop on Identity in the Browser, http://www.w3.org/2011/identity-ws/Overview.html.
4. Karsten refactored metrics-db and metrics-web by moving a lot of code from metrics-db to metrics-web (2627). metrics-db is now the tool for collecting and sanitizing metrics data, and metrics-web is the metrics website including the database schema and database import. This separation was necessary to enable people to run their own metrics-web without having to run their own metrics-db.
5. Karsten improved detection of stale bridge descriptor tarballs from Tonga by comparing descriptor publication times to tarball modification times (https://trac.torproject.org/projects/tor/ticket/2570).
6. Karsten extended BridgeDB to dump assignments to disk (https://trac.torproject.org/projects/tor/ticket/2372), wrote a script to convert old BridgeDB logs into assignment files, and extended metrics-db to sanitize these files. The files are now on the metrics website.
7. Karsten provided bridge usage data in a format that researchers can analyze much easier than the original data (https://trac.torproject.org/projects/tor/ticket/2680).
8. Karsten created a Thematic Mapping API prototype as a fancy example for visualizing Tor data (https://trac.torproject.org/projects/tor/ticket/2762).

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

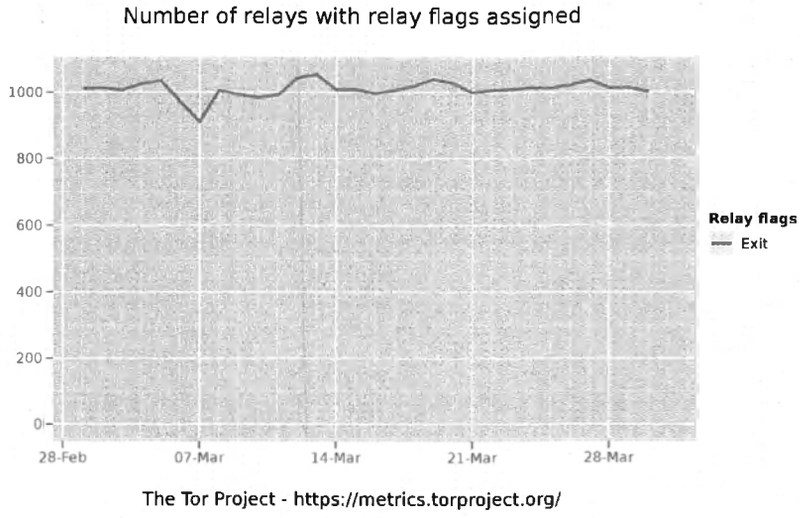
1. Karsten wrote a roadmap for the various metrics products or products that have a metrics part: metrics-web, metrics-db, ExoneraTor, VisiTor, BridgeDB, Torperf, Tor websites, bandwidth scanners, TorDNSEL, and Tor.

C.2.5. Hide Tor's network signature.

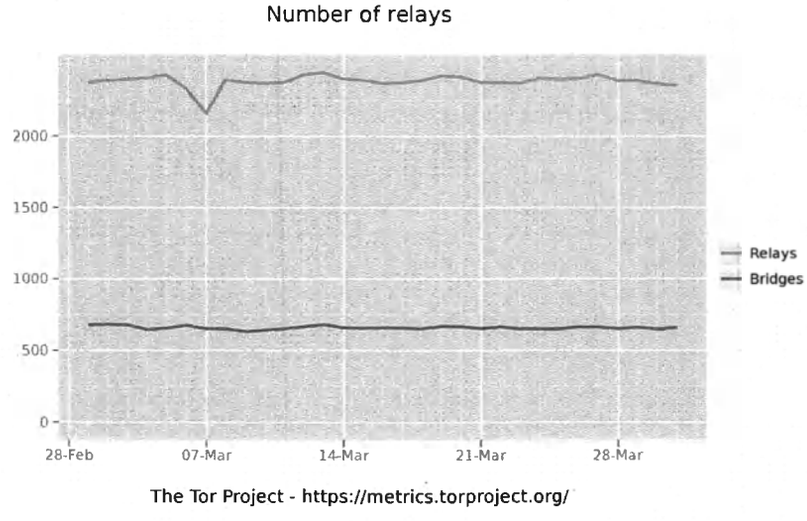
1. The pluggable transport protocol is an official proposal, number 180. https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/180-pluggable-transport.txt
2. Design updates to the TLS cert and parameter normalizations proposal, number 179, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/179-TLS-cert-and-parameter-norma txt.

C.2.10 Grow the Tor network and user base. Outreach.

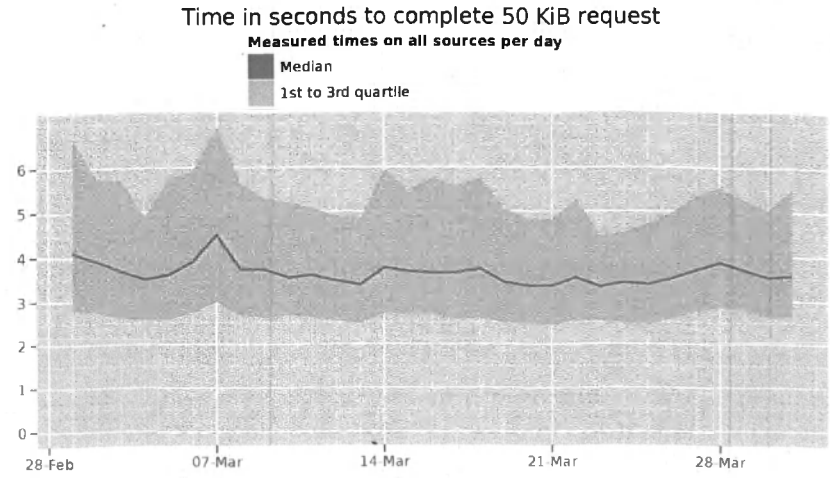
Measures of the Tor Network



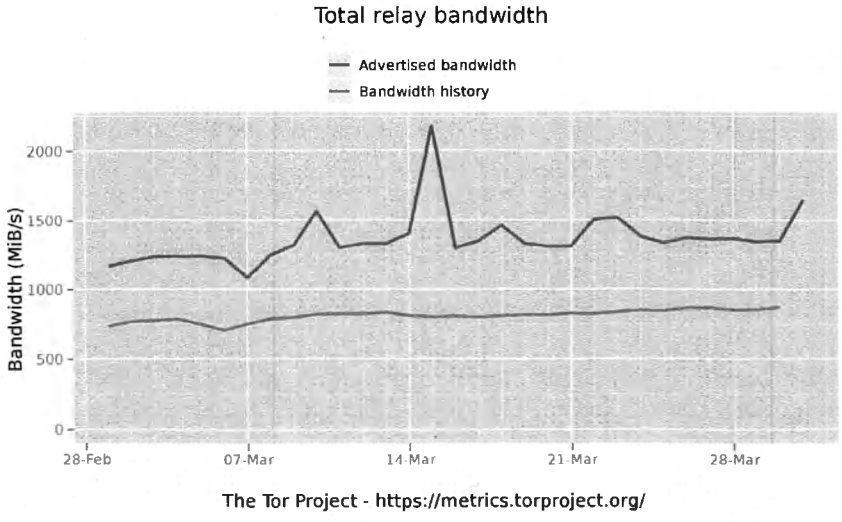
This graph shows the total quantity of exit relays in March 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graph shows the total quantity of relays and the total quantity of bridges in March 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Performance remains relatively steady at just under 4 seconds.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The steady-state of relays creates almost 1.6GBps (12.8 Gbps) of bandwidth available.

Outreach and Advocacy

1. We held a Privacy and Security Workshop at the University of London School of Oriental and African studies, `https://blog.torproject.org/blog/london-internet-security-privacy-workshop`.

2. At LibrePlanet 2011, Tor received the 2010 FSF/GNU Project Award for Project of Social Benefit. https://blog.torproject.org/blog/tor-project-receives-fsf-award.

3. Roger took a lengthy trip to Taiwan. Spoke at OSDC'11 among other locales. His trip report is at https://blog.torproject.org/blog/trip-report-taipei.

4. Andrew was interviewed by the Washington Post about US firms helping censor the Internet, http://www.washingtonpost.com/wp-dyn/content/article/2011/03/09/AR2011030905157_pf.html.

5. Wendy attended ICANN in San Francisco.

6. Andrew met with Gunilla Carlsson, the Swedish Minister of Foreign Development, and staff to discuss Tor, digital democracy, and democratic digitalization, http://www.nyteknik.se/nyheter/it_telekom/internet/article3123594.ece

7. Roger and Robert met ISI to discuss Tor and network simulation, http://www3.isi.edu/home.

8. Andrew was interviewed by Businessweek about social networking, http://www.businessweek.com/magazine/content/11_13/b4221043353206.htm

9. Erinn gave a talk at PMF (matheматički fakultet) Zagreb about Tor.

10. Erinn met with a Zagreb hackerspace, http://www.mi2.hr/, to talk about Tor.

11. Andrew was interviewed by The Telegraph to understand what's going on with Tor and Iran, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8388484/Iran-cracks-down-on-web.html

12. Jacob gave a speech at the Royal Military College of Canada, http://www.rmc.ca/

13. Andrew was featured by CNN on The Situation Room with Wolf Blitzer about US companies helping censor the Internet, http://edition.cnn.com/CNN/Programs/situation.room/

14. Nick gave a speech at the 4th Usenix Workshop on Large-scale Exploits and Emergent Threats, http://www.usenix.org/events/leet11/.

15. Tor was a finalist in the Index on Censorship New Media award, http://www.indexoncensorship.org/2011/03/free-expression-awards-2011-new-media/

16. Andrew and Karen talked to the US Senate Committee on Foreign Relations about Tor, online anonymity and privacy.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

1. TAILS nears a 0.7 release through testing of Release Candidates, http://tails.boum.org/.

2. See the "New Releases" section above for the various Tor Browser Bundles released.

C.2.12 Bridge relay and bridge authority work.

1. Torservers.net receives $10,000 to operate more bridges to support people in heavily censored areas, https://www.torservers.net/wiki/press.

2. Robert and Christian fixed a few bugs and integrated some features into the Bridge Authority codebase, https://gitweb.torproject.org/bridgedb.git/shortlog.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

1. Karsten and Mike started to design a tech report using the torperf to monitor the network through a series of experiments, the ticket list for which is here: https://trac.torproject.org/projects/tor/ticket/2769.

2. Mike did a quick review of Ian, Damon, et al's paper on their flow control and simulator work: https://lists.torproject.org/pipermail/tor-dev/2011-March/002539.html

3. Sebastian worked on libevent and Tor, to make it possible to compile them with clang with warnings. While doing so he started porting some of Tor's configure options to libevent, and fixed a few minor bugs that clang exposed.

4. Sebastian and Tomas converted Vidalia's repository from svn to git. This will allow for more distributed patches and branches.

5. Karsten reviewed and merged Mike's patch for Torperf's consolidate_stats script (https://trac.torproject.org/projects/tor/ticket/2672).

6. Karsten started writing a paper/report on Torperf and the bwscanners together with Mike (https://trac.torproject.org/projects/tor/ticket/2769). Prepared new graphs (https://trac.torproject.org/projects/tor/ticket/2772, https://trac.torproject.org/projects/tor/ticket/2394) and set up Torperfs to determine the optimal circuit build timeout cutoff (https://trac.torproject.org/projects/tor/ticket/2770).

7. Nick updates the core tor specification to include the optimistic data protocol, https://gitweb.torproject.org/torspec.git/commitdiff/ef0bff2ff3c14934a6cd056d8a9d03151741c675

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Nothing to report.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17 Translation work, ultimately a browser-based approach.

1. Runa did a bundle of work on translations, coordinating translators, and updating our various products with translations. The highlights are:

```
- updated translations from transifex (in
translation/trunk/projects/manpages/po: .tx af ak am arn ast az be bg
bn bn_IN ca cs csb cy dz el eo eu fil fur ga gl gu gun ha he hi hr ht
hu is kn kw lb ln lo lt lv mg   mi mk ml mn mr ms mt nap nb ne nl nn
nso oc pa pap pms ps pt pt_BR ro sco son su sw ta te tg th ti tk uk ur
ve vi wa zh_CN zh_HK zh_TW zu)
- updated translations from transifex for orbot (in
translation/trunk/projects/orbot/po: .tx af ak am arn ast az be bg bn
bn_IN cs csb dz el eo et eu  fil fur ga gl gu gun ha he hi hr ht id kn
kw lb ln lo lt lv     mg mi ml mn mr ms mt my nap ne nn nso oc pa pap
pms ps pt_BR ro sco son sw ta te tg th ti tk uk ve vi wa zh_HK zh_TW zu)
- updated translations from transifex for torbutton (in
translation/trunk/projects/torbutton/po: .tx af ak am arn ast be bg bn
bn_IN csb cy dz eo eu fil fur ga gl gun ha he hi ht  hu is kn kw lb
ln lo lt lv mg mi ml mn mr ms mt nap ne nn nso   oc pa pap pms ps sco
son su sw ta te tg th ti tk uk ur ve wa zh_HK zu)
- updated translations from transifex for torbutton-alpha (in
translation/trunk/projects/torbutton-alpha/po: .tx af ak am   arn
ast az be bg bn bn_IN csb cy dz eo eu fil fur ga gl gun     ha he ht
hu is kn kw lb ln lo lt lv mg mi mk ml mn mr ms mt nap ne nn nso
oc pa pap pms ps sco son su sw ta te tg ti tk    ur ve wa zh_HK zu)
- updated translations from transifex for torcheck (in
translation/trunk/projects/torcheck/po: .tx af ak am arn ast  az bg
bn_IN csb de_CH dz eo eu fil fur ga gu gun ha he hr ht    is kn lb ln
lo lt lv mg mi ml mn mr ms mt nah nap ne nn nso     oc pa pap pms ps
sco son su ta te tg ti tk ur ve zh_HK zu)
- updated translations from transifex for the website (in
translation/trunk/projects/website/po: .tx zh_CN/about)
- updated translations for vidalia (in vidalia/trunk/src/vidalia/i18n/po:
.tx af ak am arn ast az be   bg bn bn_IN bo br bs ca csb cy de_CH de_DE
dz et eu fil fo      fur fy ga gl gun ha hi hr ht hy is jv ka km kn
ko ku kw ky lb   ln lo lt lv mg mi mk ml mn mr ms mt nah nap ne nn nso
oc or    pa pap pms ps sco sk so son st su sw ta te tg th ti tk uk ur
ve vi wa wo zh_HK zu)
- updated translations for vidaliahelp (in
vidalia/trunk/src/vidalia/help/content/po: .tx af ak am arn ast az be
bg bn bn_IN ca cs csb cy dz el eo et eu fil fur ga    gl gu gun ha he
hi hr ht hu id is kn kw lb ln lo lt lv mg mi  mk ml mn mr ms mt nap
nb ne nl nn nso oc pa pap pms ps pt ro    sco son su sw ta te tg th ti
tk tr uk ur ve vi wa zh_HK zh_TW zu)
- updated translations for vidalia installer (in
vidalia/trunk/pkg/win32/po: .tx af ak am arn ast bg bn_IN csb  cy
de_CH dz eo eu fil fur ga gl gu gun ha hi hr ht hu is kn     lb ln lo
lt lv mg mi mk ml mn mr ms mt nah nap ne nn nso oc pa pap pms ps
pt_BR sco son su sw ta te tg ti tk ur ve zh_HK zu)
- translations for vidaliahelp as html files (in
```

```
vidalia/trunk/src/vidalia/help/content: . my zh_CN)
```

June 14, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-seventh invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at [redacted] if there are any questions.

Invoice 37:

Period	Months	Rate	Cost
04/17/2011 - 05/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG06142011

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: June 8, 2011

This report documents progress in May 2011 on contract BBGCON1807S6441 between BBG and The Tor Project.

New releases, new hires, new funding

New Hires

RiseUp Labs have been contracted to enhance and improve the TAILS anonymous operating system, `http://tails.boum.org`.

New Releases

1. On May 5 we released a new highly experimental branch of Tor, 0.2.3.1-alpha. Tor 0.2.3.1-alpha adds some new experimental features, including support for an improved network IO backend, IOCP networking on Windows, microdescriptor caching, "fast-start" support for streams, and automatic home router configuration. There are also numerous internal improvements to try to make the code easier for developers to work with.

   This is the first alpha release in a new series, so expect there to be bugs. Users who would rather test out a more stable branch should stay with 0.2.2.x for now. For now, only the source has been uploaded. Our website scripts don't like for there to be three active branches at one time, so while we're getting that straightened out, you can get the source and the signature at `https://www.torproject.org/dist/tor-0.2.3.1-alpha.tar.gz` and `https://www.torproject.org/dist/tor-0.2.3.1-alpha.tar.gz.asc` respectively. Packages for Debian and expert packages for other platforms should follow. If you don't build from source, and prefer the easier-to-use packages, please stick with 0.2.2.x or 0.2.1.x until we get more bugs shaken out of this one.

```
o Major features
  - Tor can now optionally build with the "bufferevents" buffered IO
    backend provided by Libevent 2. To use this feature, make sure you
    have the latest possible version of Libevent, and pass the
    --enable-bufferevents flag to configure when building Tor from
    source. This feature will make our networking code more flexible,
    let us stack layers on each other, and let us use more efficient
    zero-copy transports where available.
  - As an experimental feature, Tor can use IOCP for networking on Windows.
```

Once this code is tuned and optimized, it promises much better performance than the select-based backend we've used in the past. To try this feature, you must build Tor with Libevent 2, configure Tor with the "bufferevents" buffered IO backend, and add "DisableIOCP 0" to your torrc. There are known bugs here: only try this if you can help debug it as it breaks.

- The EntryNodes option can now include country codes like {de} or IP addresses or network masks. Previously we had disallowed these options because we didn't have an efficient way to keep the list up to date. Fixes bug 1982, but see bug 2798 for an unresolved issue here.
- Exit nodes now accept and queue data on not-yet-connected streams. Previously, the client wasn't allowed to send data until the stream was connected, which slowed down all connections. This change will enable clients to perform a "fast-start" on streams and send data without having to wait for a confirmation that the stream has opened. (Patch from Ian Goldberg; implements the server side of Proposal 174.)
- Tor now has initial support for automatic port mapping on the many home routers that support NAT-PMP or UPnP. (Not yet supported on Windows). To build the support code, you'll need to have libnatpnp library and/or the libminiupnpc library, and you'll need to enable the feature specifically by passing "--enable-upnp" and/or "--enable-natpnp" to configure. To turn it on, use the new PortForwarding option.
- Caches now download, cache, and serve multiple "flavors" of the consensus, including a flavor that describes microdescriptors.
- Caches now download, cache, and serve microdescriptors -- small summaries of router descriptors that are authenticated by all of the directory authorities. Once enough caches are running this code, clients will be able to save significant amounts of directory bandwidth by downloading microdescriptors instead of router descriptors.

o Minor features:

- Make logging resolution configurable with a new LogGranularity option, and change the default from 1 millisecond to 1 second. Implements enhancement 1668.
- We log which torrc file we're using on startup. Implements ticket 2444.
- Ordinarily, Tor does not count traffic from private addresses (like 127.0.0.1 or 10.0.0.1) when calculating rate limits or accounting. There is now a new option, CountPrivateBandwidth, to disable this behavior. Patch from Daniel Cagara.
- New --enable-static-tor configure option for building Tor as statically as possible. Idea, general hackery and thoughts from Alexei Czeskis, John Gilmore, Jacob Appelbaum. Implements ticket 2702.

- If you set the NumCPUs option to 0, Tor will now try to detect how many CPUs you have. This is the new default behavior.
- Turn on directory request statistics by default and include them in extra-info descriptors. Don't break if we have no GeoIP database.
- Relays that set "ConnDirectionStatistics 1" write statistics on the bidirectional use of connections to disk every 24 hours.
- Add a GeoIP file digest to the extra-info descriptor. Implements enhancement 1883.
- Add a new 'Heartbeat' log message type to periodically log a message describing Tor's status at level Notice. This feature is meant for operators who log at notice, and want to make sure that their Tor server is still working. Implementation by George Kadianakis.

o Minor bugfixes (on 0.2.2.25-alpha):
- When loading the microdesc journal, remember its current size. In 0.2.2, this helps prevent the microdesc journal from growing without limit on authorities (who are the only ones to use it in 0.2.2). Fixes a part of bug 2230; bugfix on 0.2.2.6-alpha. Fix posted by "cypherpunks."
- The microdesc journal is supposed to get rebuilt only if it is at least _half_ the length of the store, not _twice_ the length of the store. Bugfix on 0.2.2.6-alpha; fixes part of bug 2230.
- If as an authority we fail to compute the identity digest of a v3 legacy keypair, warn, and don't use a buffer-full of junk instead. Bugfix on 0.2.1.1-alpha; fixes bug 3106.
- Authorities now clean their microdesc cache periodically and when reading from disk initially, not only when adding new descriptors. This prevents a bug where we could lose microdescriptors. Bugfix on 0.2.2.6-alpha.

o Minor features (controller)
- Add a new SIGNAL event to the controller interface so that controllers can be notified when Tor handles a signal. Resolves issue 1955. Patch by John Brooks.
- Add a new GETINFO option to get total bytes read and written. Patch from pipe, revised by atagar. Resolves ticket 2345.
- Implement some GETINFO controller fields to provide information about the Tor process's pid, euid, username, and resource limits.

o Build changes
- Our build system requires automake 1.6 or later to create the Makefile.in files. Previously, you could have used 1.4. This only affects developers and people building Tor from git; people who build Tor from the source distribution without changing the Makefile.am files should be fine.

```
    - Our autogen.sh script uses autoreconf to launch autoconf, automake, and
      so on. This is more robust against some of the failure modes
      associated with running the autotools pieces on their own.

  o Minor packaging issues:
    - On OpenSUSE, create the /var/run/tor directory on startup if it is not
      already created. Patch from Andreas Stieger. Fixes bug 2573.

  o Code simplifications and refactoring:
    - A major revision to our internal node-selecting and listing logic.
      Tor already had at least two major ways to look at the question of
      "which Tor servers do we know about": a list of router descriptors,
      and a list of entries in the current consensus. With
      microdescriptors, we're adding a third. Having so many systems
      without an abstraction layer over them was hurting the codebase.
      Now, we have a new "node_t" abstraction that presents a consistent
      interface to a client's view of a Tor node, and holds (nearly) all
      of the mutable state formerly in routerinfo_t and routerstatus_t.
    - The helper programs tor-gencert, tor-resolve, and tor-checkkey
      no longer link against Libevent: they never used it, but
      our library structure used to force them to link it.

  o Removed features:
    - Remove some old code to work around even older versions of Tor that
      used forked processes to handle DNS requests. Such versions of Tor
      are no longer in use as servers.

  o Documentation fixes:
    - Correct a broken faq link in the INSTALL file. Fixes bug 2307.
    - Add missing documentation for the authority-related torrc options
      RephistTrackTime, BridgePassword, and V3AuthUseLegacyKey. Resolves
      issue 2379.
```

2. On May 9, an updated Orbot, Tor for Android, was released for testing. Based on feedback from our core test group in the Guardian Project, it seems like we have a solid new version of Orbot that includes Tor 0.2.2.25, as well as improved handling of transparent proxying. This new build also includes our own version of iptables, and proactively checks if the device has netfilter/owner support in the kernel. This should lead to overall less support requests from confused users who have "root" but still can't transproxy.

   We have a few UI tweaks to make, and need to make sure all of our translations are up-to-date, but otherwise, the app feels very ready to go.

   I invite any of you with a few spare cycles and an Android device handy to try it out if you haven't already. As this is a dev build, it is not signed by the official Tor distro key, so you will have to uninstall any existing Orbot official release. The final app we release to the market will be signed by the Tor key, and users will get an automatic "updates available"

message from the Android market.

The software is available at `https://guardianproject.info/downloads/0.2.2.25-orbot-alpha-1.0.5.20110508a-dev.apk` with the (.asc - signed by [redacted] 0xB374CBD2)

3. On May 6, we released an experimental Vidalia branch, 0.3.0. We are going to be doing a series of alpha releases in parallel with the stable 0.2.x to have a wider audience for some changes that are kind of "core" for Vidalia, or they are really big to put them on the stable before testing them for a while.

   We need more eyes, but I want to be clear about the "alpha" part in the version. The bundles that were just announced they also have an alpha version of Tor, the latest libevent, the latest openssl, and so on, not just this Vidalia release. So be aware of this while running them.

```
0.3.0  06-May-2011
  o Vidalia has got a new GUI. Instead of separate dialogs, each
    functionality is organized in tabs arranged in a common main window.
    This new tab organization will give Vidalia a generic way of
    organizing the GUI plug-ins that will be available in later
    releases.  Resolves bug 2939.
  o When a Tor instance is already running and Vidalia doesn't know the
    control password, don't ask for the it but rather explain the
    situation and display the few possible choices the user has.
    Resolves bug 2132.
  o Add an option for setting up a non-exit relay to the Sharing
    configuration panel. This is meant to clarify what an exit policy
    and an exit relay are.  Resolves bug 2644.
  o Add a way to reload Tor's configuration without having to stop it.
    Tor can reload its configuration while it is running, Vidalia now
    provides a menu option for that, so, for example, relay operators
    won't be affected by the fact that their relay was down for a while.
    Resolves bug 2724.
  o Reintegrate Breakpad, and make available in other platforms other
    than Windows. Resolves bug 2105.
  o Fix bandwidth assigned to relays on the Network Map. A lot of relays
    are displaying an erroneous bandwidth and since they are ordered by
    that value in the Network Map, it leads to confusion. Vidalia now
    specifies the bandwidth as the minimum of the three possible values
    (burst, average and observed). Fixes bug 2744.
  o Minor change to the checkbox for starting Tor when Vidalia starts.
    It was suggested that the way the phrasing was done was missleading.
    Resolves bug 2806.
  o Add a way to bootstrap Tor's torrc file (copy the torrc to a given
    directory before Vidalia starts) so that packages such as
    Bridge-by-default portable bundles for OSX don't violate the
    directory structure of the operative system. Fixes bug 2821.
  o Add the proper CA Certificates so that the "Find Bridges" button
```

```
    works again. Fixes bug 2835.
  o Update the useful links help page. Fixes bug 2809.
```

4. On May 11, we released some experimental Vidalia bundles containing Vidalia 0.3.0-alpha and Tor 0.2.3.1-alpha.

```
OS X, 10.5 and 10.6 only (untested on 10.5, please let me know if it works):
https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3
https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3

Windows XP through Win7 (might work on Win2k, can someone test and confirm?):
https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3
https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3
```

5. On May 17, we released Tor 0.2.2.26-beta. Tor 0.2.2.26-beta fixes a variety of potential privacy problems. It also introduces a new "socksport auto" approach that should make it easier to run multiple Tors on the same system, and does a lot of cleanup to get us closer to a release candidate.

```
  o Security/privacy fixes:
    - Replace all potentially sensitive memory comparison operations
      with versions whose runtime does not depend on the data being
      compared. This will help resist a class of attacks where an
      adversary can use variations in timing information to learn
      sensitive data. Fix for one case of bug 3122. (Safe memcmp
      implementation by Robert Ransom based partially on code by DJB.)
    - When receiving a hidden service descriptor, check that it is for
      the hidden service we wanted. Previously, Tor would store any
      hidden service descriptors that a directory gave it, whether it
      wanted them or not. This wouldn't have let an attacker impersonate
      a hidden service, but it did let directories pre-seed a client
      with descriptors that it didn't want. Bugfix on 0.0.6.
    - On SIGHUP, do not clear out all TrackHostExits mappings, client
      DNS cache entries, and virtual address mappings: that's what
      NEWNYM is for. Fixes bug 1345; bugfix on 0.1.0.1-rc.

  o Major features:
    - The options SocksPort, ControlPort, and so on now all accept a
      value "auto" that opens a socket on an OS-selected port. A
      new ControlPortWriteToFile option tells Tor to write its
      actual control port or ports to a chosen file. If the option
      ControlPortFileGroupReadable is set, the file is created as
      group-readable. Now users can run two Tor clients on the same
```

system without needing to manually mess with parameters. Resolves part of ticket 3076.
- Set SO_REUSEADDR on all sockets, not just listeners. This should help busy exit nodes avoid running out of useable ports just because all the ports have been used in the near past. Resolves issue 2850.

o Minor features:
- New "GETINFO net/listeners/(type)" controller command to return a list of addresses and ports that are bound for listeners for a given connection type. This is useful when the user has configured "SocksPort auto" and the controller needs to know which port got chosen. Resolves another part of ticket 3076.
- Add a new ControlSocketsGroupWritable configuration option: when it is turned on, ControlSockets are group-writeable by the default group of the current user. Patch by JÃ©rÃ©my Bobbio; implements ticket 2972.
- Tor now refuses to create a ControlSocket in a directory that is world-readable (or group-readable if ControlSocketsGroupWritable is 0). This is necessary because some operating systems do not enforce permissions on an AF_UNIX sockets. Permissions on the directory holding the socket, however, seems to work everywhere.
- Rate-limit a warning about failures to download v2 networkstatus documents. Resolves part of bug 1352.
- Backport code from 0.2.3.x that allows directory authorities to clean their microdescriptor caches. Needed to resolve bug 2230.
- When an HTTPS proxy reports "403 Forbidden", we now explain what it means rather than calling it an unexpected status code. Closes bug 2503. Patch from Michael Yakubovich.
- Update to the May 1 2011 Maxmind GeoLite Country database.

o Minor bugfixes:
- Authorities now clean their microdesc cache periodically and when reading from disk initially, not only when adding new descriptors. This prevents a bug where we could lose microdescriptors. Bugfix on 0.2.2.6-alpha. 2230
- Do not crash when our configuration file becomes unreadable, for example due to a permissions change, between when we start up and when a controller calls SAVECONF. Fixes bug 3135; bugfix on 0.0.9pre6.
- Avoid a bug that would keep us from replacing a microdescriptor cache on Windows. (We would try to replace the file while still holding it open. That's fine on Unix, but Windows doesn't let us do that.) Bugfix on 0.2.2.6-alpha; bug found by wanoskarnet.
- Add missing explanations for the authority-related torrc options

RephistTrackTime, BridgePassword, and V3AuthUseLegacyKey in the man page. Resolves issue 2379.
- As an authority, do not upload our own vote or signature set to ourself. It would tell us nothing new, and as of 0.2.2.24-alpha, it would get flagged as a duplicate. Resolves bug 3026.
- Accept hidden service descriptors if we think we might be a hidden service directory, regardless of what our consensus says. This helps robustness, since clients and hidden services can sometimes have a more up-to-date view of the network consensus than we do, and if they think that the directory authorities list us a HSDir, we might actually be one. Related to bug 2732; bugfix on 0.2.0.10-alpha.
- When a controller changes TrackHostExits, remove mappings for hosts that should no longer have their exits tracked. Bugfix on 0.1.0.1-rc.
- When a controller changes VirtualAddrNetwork, remove any mappings for hosts that were automapped to the old network. Bugfix on 0.1.1.19-rc.
- When a controller changes one of the AutomapHosts* options, remove any mappings for hosts that should no longer be automapped. Bugfix on 0.2.0.1-alpha.
- Do not reset the bridge descriptor download status every time we re-parse our configuration or get a configuration change. Fixes bug 3019; bugfix on 0.2.0.3-alpha.

o Minor bugfixes (code cleanup):
- When loading the microdesc journal, remember its current size. In 0.2.2, this helps prevent the microdesc journal from growing without limit on authorities (who are the only ones to use it in 0.2.2). Fixes a part of bug 2230; bugfix on 0.2.2.6-alpha. Fix posted by "cypherpunks."
- The microdesc journal is supposed to get rebuilt only if it is at least _half_ the length of the store, not _twice_ the length of the store. Bugfix on 0.2.2.6-alpha; fixes part of bug 2230.
- Fix a potential null-pointer dereference while computing a consensus. Bugfix on tor-0.2.0.3-alpha, found with the help of clang's analyzer.
- Avoid a possible null-pointer dereference when rebuilding the mdesc cache without actually having any descriptors to cache. Bugfix on 0.2.2.6-alpha. Issue discovered using clang's static analyzer.
- If we fail to compute the identity digest of a v3 legacy keypair, warn, and don't use a buffer-full of junk instead. Bugfix on 0.2.1.1-alpha; fixes bug 3106.
- Resolve an untriggerable issue in smartlist_string_num_isin(), where if the function had ever in the future been used to check

```
    for the presence of a too-large number, it would have given an
    incorrect result. (Fortunately, we only used it for 16-bit
    values.) Fixes bug 3175; bugfix on 0.1.0.1-rc.
  - Require that introduction point keys and onion handshake keys
    have a public exponent of 65537. Starts to fix bug 3207; bugfix
    on 0.2.0.10-alpha.

o Removed features:
  - Caches no longer download and serve v2 networkstatus documents
    unless FetchV2Networkstatus flag is set: these documents haven't
    haven't been used by clients or relays since 0.2.0.x. Resolves
    bug 3022.
```

6. On May 18, we released Tor 0.2.2.27-beta. Tor 0.2.2.27-beta fixes a bridge-related stability bug in the previous release, and also adds a few more general bugfixes.

```
o Major bugfixes:
  - Fix a crash bug when changing bridges in a running Tor process.
    Fixes bug 3213; bugfix on 0.2.2.26-beta.
  - When the controller configures a new bridge, don't wait 10 to 60
    seconds before trying to fetch its descriptor. Bugfix on
    0.2.0.3-alpha; fixes bug 3198 (suggested by 2355).

o Minor bugfixes:
  - Require that onion keys have exponent 65537 in microdescriptors too.
    Fixes more of bug 3207; bugfix on 0.2.2.26-beta.
  - Tor used to limit HttpProxyAuthenticator values to 48 characters.
    Changed the limit to 512 characters by removing base64 newlines.
    Fixes bug 2752. Fix by Michael Yakubovich.
  - When a client starts or stops using bridges, never use a circuit
    that was built before the configuration change. This behavior could
    put at risk a user who uses bridges to ensure that her traffic
    only goes to the chosen addresses. Bugfix on 0.2.0.3-alpha; fixes
    bug 3200.
```

7. On May 23, we released updated packages for Linux, OS X, and Microsoft Windows. All of the alpha Tor Browser Bundles have been updated to the latest Tor 0.2.2.27-beta.

```
Firefox 3.6 Tor Browser Bundles
Linux bundles
1.1.9: Released 2011-05-19
Update Tor to 0.2.2.27-beta
Update NoScript to 2.1.0.5
Update BetterPrivacy to 1.50
Update HTTPS Everywhere to 0.9.9.development.5
```

```
OS X bundle
1.0.17: Released 2011-05-19
Update Tor to 0.2.2.27-beta
Update NoScript to 2.1.0.5
Update HTTPS-Everywhere to 0.9.9.development.5
Update BetterPrivacy to 1.50

Firefox 4 Tor Browser Bundles
Tor Browser Bundle (2.2.27-1)
Update Tor to 0.2.2.27-beta
Update HTTPS Everywhere to 0.9.9.development.5
Update NoScript to 2.1.0.5
```

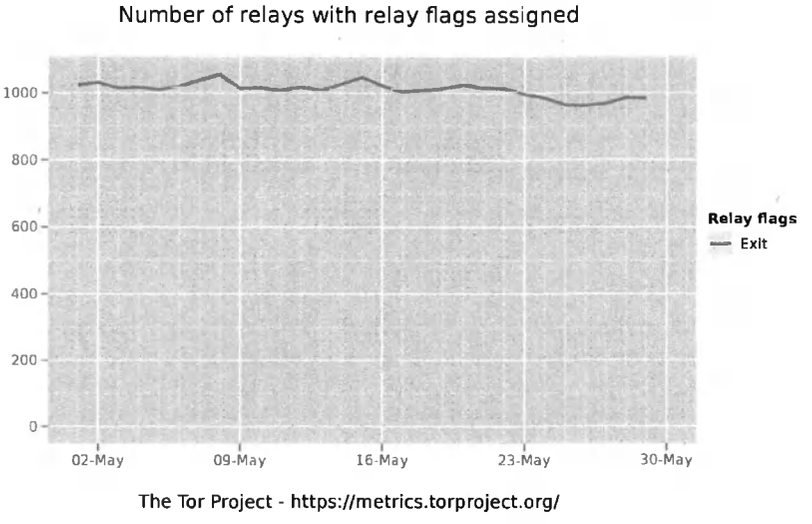
Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- Nick spent a while chasing security issues, particularly bug 3122, `https://trac.torproject.org/projects/tor/ticket/3122`. This should make Tor more resilient to a class of timing attack. In practice, we still doubt whether there could be exploitable bugs here: we believe that getting good enough answers to mount a good timing attack would require that Tor be a lot less noisy in its current timing behavior. Nonetheless, we could be quite wrong.
- Nick and George started writing out the threat models and specification for obfsproxy, `https://gitweb.torproject.org/obfsproxy.git/tree/HEAD:/doc`.

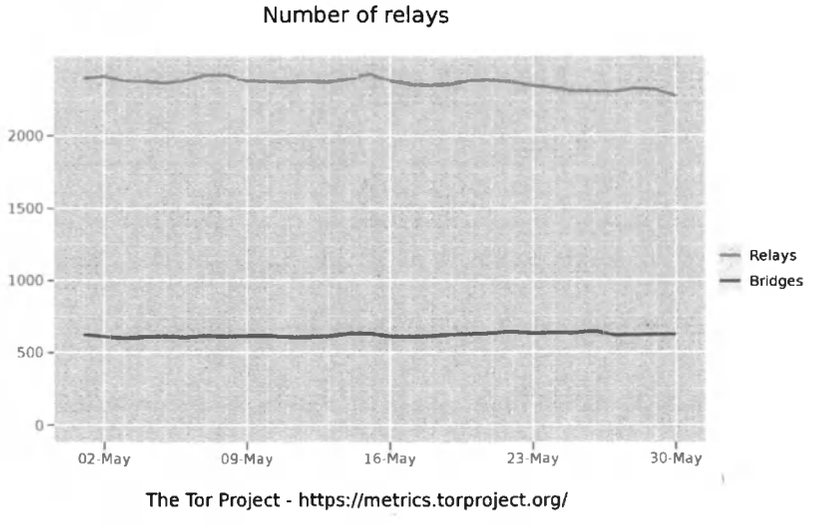
Hide Tor's network signature.

Grow the Tor network and user base. Outreach.

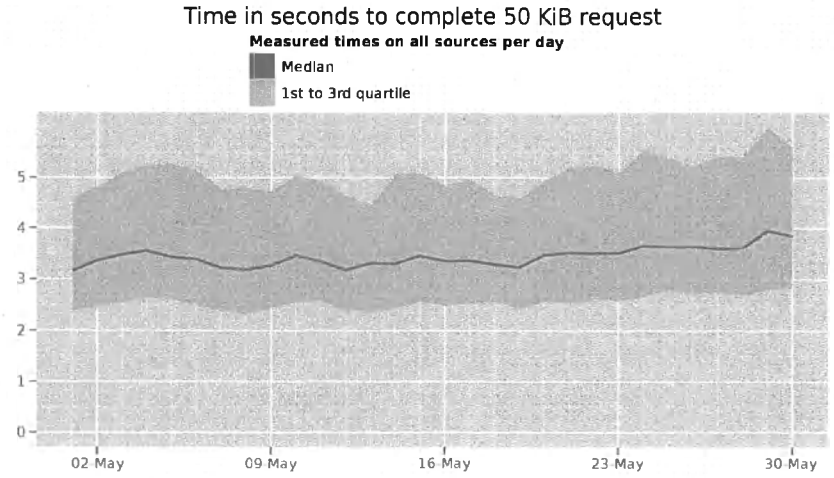
Measures of the Tor Network



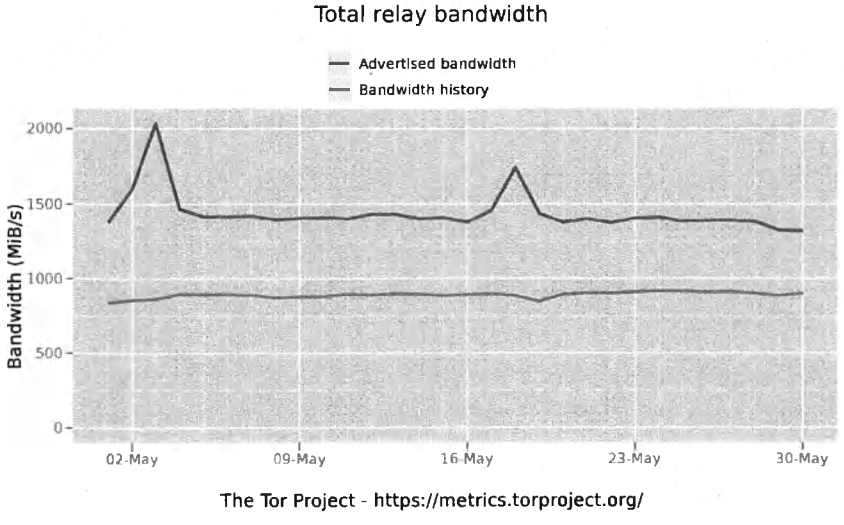
This graph shows the total quantity of exit relays in May 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graph shows the total quantity of relays and the total quantity of bridges in May 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Performance remains relatively steady at just under 4 seconds.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The steady-state of relays creates almost 1.5GBps (12.0 Gbps) of bandwidth available.

Outreach and Advocacy

1. Andrew spoke at World Press Freedom Day, `http://www.wpfd2011.org/`. His presentation is available here `https://svn.torproject.org/svn/projects/presentations/2011-WorldPressFreedomDa`

pdf.

2. Jacob attended Google I/O, http://www.google.com/events/io/2011/.
3. Andrew traveled to Iceland to meet with the International Modern Media Institute, National Police of Iceland, and Hakkavélin. His trip report was published as a blog post, https://blog.torproject.org/blog/visit-iceland.
4. Andrew, Runa, Sebastian, George, and Linus worked with IIS.se to hold a successful hackfest in Stockholm, https://blog.torproject.org/blog/2011-stockholm-hackfest-thanks. IIS further published the event in Swedish at https://www.iis.se/blogg/hackare-intar-se and their follow-up, https://www.iis.se/internet-for-alla/reportage/teknikreportage/hackare-intog-se.
5. Andrew and Runa met with University College of London Information Security Research Group, http://sec.cs.ucl.ac.uk/. Andrew presented about usability, humans, and Tor with this presentation, https://svn.torproject.org/svn/projects/presentations/2011-anonymity-us pdf.
6. Andrew and Dr. Angela Sasse from UCL were interviewed by the BBC Click program about why Internet Anonymity is important and valuable in a modern, networked society. http://news.bbc.co.uk/2/hi/programmes/click_online/default.stm
7. Mike spoke at W3C Identity, http://www.w3.org/2011/identity-ws/Overview.html and presented this paper, https://svn.torproject.org/svn/projects/articles/browser-privacy/.
8. Mike attended Web 2.0 Security and Privacy, http://w2spconf.com/2011/.
9. Roger attended the IEEE Symposium on Security and Privacy, http://www.ieee-security.org/TC/SP2011/index.html.
10. Runa attended the Youth Congress on Digital Citizenship in London, http://www.cybersummit2011.com/.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Bridge relay and bridge authority work.

- Runa continued to work on the Excito web interface, and sent Excito the text for the help page. The current iteration of the interface looks like this http://forum.excito.net/download/file.php?id=91.
- Runa went to Malmö, Sweden to meet and work with developers at Excito. The trip was successful in getting the Tor parts of the web interface integrated into the rest of the B3 management interface.
- Runa received a DreamPlug from GlobalScale Technologies. The idea was that this plug could be used for the Torouter project. It may not be as user friendly as first thought. See "The Torouter and the DreamPlug" on tor-dev for more info., https://lists.torproject.org/pipermail/tor-dev/2011-May/002686.html.

- Roger put up a 'need more bridge addresses' blog post, and managed some of the comments: https://blog.torproject.org/blog/strategies-getting-more-bridge-addresses

Scalability, load balancing, directory overhead, efficiency.

- Nick had some pretty good discussions about possibilities for faster ECC-based handshakes on or-dev, turning Goldberg Stebila and Ustaoglu's design into a spec proposal idea draft. We'd like to see about getting this into a release; it seems like it would make circuit crypto much faster.

- From the 0.2.3.0 release notes: As an experimental feature, Tor can use IOCP for networking on Windows. Once this code is tuned and optimized, it promises much better performance than the select-based backend we've used in the past. To try this feature, you must build Tor with Libevent 2, configure Tor with the "bufferevents" buffered IO backend, and add "DisableIOCP 0" to your torrc. There are known bugs here: only try this if you can help debug it as it breaks.

- From the 0.2.3.0 release notes: Exit nodes now accept and queue data on not-yet-connected streams.Previously, the client wasn't allowed to send data until the stream was connected, which slowed down all connections. This change will enable clients to perform a "fast-start" on streams and send data without having to wait for a confirmation that the stream has opened. (Patch from Ian Goldberg; implements the server side of Proposal 174.)

- From the 0.2.3.0 release notes: Tor now has initial support for automatic port mapping on the many home routers that support NAT-PMP or UPnP. (Not yet supported on Windows). To build the support code, you'll need to have libnatpnp library and/or the libminiupnpc library, and you'll need to enable the feature specifically by passing "–enable-upnp" and/or "–enable-natpnp" to configure. To turn it on, use the new PortForwarding option.

- Steven is writing a comparison of datagram protocols for Tor. Current draft of the comparison is available at https://gitweb.torproject.org/sjm217/torspec.git/tree/refs/heads/datagram_comparison:/proposals/ideas/xxx-datagram-comparison. Updated progress at https://trac.torproject.org/projects/tor/ticket/1855.

- Tor 0.2.3.1-alpha was released which includes full microdescriptor client and relay support. Progress is being tracked at https://trac.torproject.org/projects/tor/ticket/1748. Specific changelog entries available at https://lists.torproject.org/pipermail/tor-talk/2011-May/020313.html. Relevant entries are:

```
  - Caches now download, cache, and serve microdescriptors -- small
    summaries of router descriptors that are authenticated by all of the
    directory authorities. Once enough caches are running this code,
    clients will be able to save significant amounts of directory bandwidth
    by downloading microdescriptors instead of router descriptors.

  o Minor bugfixes (on 0.2.2.25-alpha):
  - When loading the microdesc journal, remember its current size.
```

```
    In 0.2.2, this helps prevent the microdesc journal from growing
    without limit on authorities (who are the only ones to use it in
    0.2.2). Fixes a part of bug 2230; bugfix on 0.2.2.6-alpha.
    Fix posted by "cypherpunks."
  - The microdesc journal is supposed to get rebuilt only if it is
    at least _half_ the length of the store, not _twice_ the length
    of the store. Bugfix on 0.2.2.6-alpha; fixes part of bug 2230.
  - If as an authority we fail to compute the identity digest of a v3
    legacy keypair, warn, and don't use a buffer-full of junk instead.
    Bugfix on 0.2.1.1-alpha; fixes bug 3106.
  - Authorities now clean their microdesc cache periodically and when
    reading from disk initially, not only when adding new descriptors.
    This prevents a bug where we could lose microdescriptors. Bugfix
    on 0.2.2.6-alpha.
```

- Bandwidth authority improvements.
  - ticket 2391 'upgrade to use new sqlalchemy and elixir:' completed. https://trac.torproject.org/projects/tor/ticket/2391
  - ticket 2392 'support postgres/mysql backend': completed, but fix for 2947 conflicts. Seeking resolution. https://trac.torproject.org/projects/tor/ticket/2392
  - ticket 2550 'bwauth should reschedule quicker bandwidth test when bandwidthrate changes?' - part a. implemented. Waiting on feedback from Mike to determine if we are proceeding with parts b. and c. https://trac.torproject.org/projects/tor/ticket/2550
  - ticket 2568 'IOError: file name too long' - completed. implemented a fix, but unable to reproduce the bug – possibly an OS bug. (see ticket for details: https://trac.torproject.org/projects/tor/ticket/2568)
  - ticket 2947 - 'bwscanner does not clear stream data between slices' Fixed but hasn't had the impact that Mike I were hoping for. 2 weeks of testing show improvement in memory usage but usage continues to grow. The sqlite database is only about 5MB in size, so it looks like the memory leak is elsewhere. https://trac.torproject.org/projects/tor/ticket/2947

Incentives work.

Nothing to report.

More reliable (e.g. split) download mechanism.

To great effect the world over, Mike blogged about ending torbutton as a separate entity and forking Firefox. https://blog.torproject.org/blog/toggle-or-not-toggle-end-torbutton. This story was reported upon by at least 30 different media outlets around the world.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- updated the translation template for Orbot and pushed/pulled new translations: `https://trac.torproject.org/projects/tor/ticket/3104`.
- pulled and validated translations for Vidalia, Vidalia Installer, the Vidalia help files and the website.
- created a Vidalia-alpha resource on Transifex and added the translations we have right now (they are currently the same as for the stable version of Vidalia): `https://trac.torproject.org/projects/tor/ticket/3092`.
- The German translation of overview.html contained wml code. Fixed it by closing a couple of tags: `https://trac.torproject.org/projects/tor/ticket/3102`.
- The Russian translation of overview.html didn't include the sidenav. Fixed by removing extra space before one of the include lines: `https://trac.torproject.org/projects/tor/ticket/3120`.

November 15, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our 42nd invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at [redacted] if there are any questions.

Invoice 42:

Period	Months	Rate	Cost
09/17/2011 - 10/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG11152011

From: Andrew Lewman, Executive Director
To: The Tor Community
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: November 8, 2011

This report documents progress in October 2011 on contract BBGCON1807S6441 between BBG and The Tor Project.

New releases, new hires, new funding

New Releases

1. On October 7th, we released a new version of Vidalia, version 0.2.15. The detailed changelog is below:

```
0.2.15 07-Oct-2011

    Draw the bandwidth graph curves based on the local maximum, not
    the global maximum. Fixes bug 2188.
    Add an option for setting up a non-exit relay to the Sharing
    configuration panel. This is meant to clarify what an exit policy
    and an exit relay are. Resolves bug 2644.
    Display time statistics for bridges in UTC time, rather than local
    time. Fixes bug 3342.
    Change the parameter for ordering the entries in the Basic Log
    list from currentTime to currentDateTime to avoid missplacing
    entries from different days.
    Check the tor version and that settings are sanitized before
    trying to use the port autoconfiguration feature. Fixes bug 3843.
    Provide a way to hide Dock or System Tray icons in OSX. Resolves
    ticket 2163.
    Make new processes appear at front when they are started (OSX
    specific).
```

2. On October 12th, we released updated tor browser bundles.

   The Tor Browser Bundles have been updated to Vidalia 0.2.15. The OS X and Linux bundles have Torbutton 1.4.4, but a hotfix for Windows was released with 1.4.4.1 because 1.4.4 had a minor issue that prevented the Windows bundle from going to https://check.torproject.org.

```
Tor Browser Bundle (2.2.33-3)
```

```
Update Vidalia to 0.2.15
Update Torbutton to 1.4.4.1
Update NoScript to 2.1.4
Remove trailing dash from Windows version number (closes: #4160)
Make Tor Browser (Aurora) fail closed when not launched with a TBB profile
(closes: #4192)
```

3. On October 16th, the Tails Live System version 0.8.1 was released. Detailed changes are:

```
* Iceweasel
  - Update to 3.5.16-10 (fixes DSA-2313-1).
  - FireGPG: force crypto action results to appear in a new window, otherwise
    JavaScript can steal decrypted plaintext. Advice: always use FireGPG's
    text editor when writing text you want to encrypt. If you write it in a
    textbox the plaintext can be stolen through JavaScript before it is
    encrypted in the same way.
  - Update HTTPS Everywhere extension to 1.0.3-1.
  - Stop using the small version of the Tor check page. The small version
    incorrectly tells Tails users to upgrade their Torbrowser, which has
    confused some users.

* Software
  - Update Linux to 3.0.0-2 (fixes DSA-2310-1, CVE-2011-2905, CVE-2011-2909,
    CVE-2011-2723, CVE-2011-2699, CVE-2011-1162, CVE-2011-1161).
  - Update usb-modeswitch to 1.1.9-2~bpo60+1 and usb-modeswitch-data to
    20110805-1~bpo60+1 from Debian backports. This adds support for a few
    devices such as Pantech UMW190 CDMA modem.
  - Install libregexp-common-perl 2011041701-3 from Debian unstable. This
    fixes the bug: [[bugs/msva_does_not_use_configured_keyserver]].
  - Install hdparm so the hard drives can be spinned down in order to save
    battery power.
  - Install barry-util for better BlackBerry integration.
  - Debian security upgrades: OpenOffice.org (DSA-2315-1), openjdk-6
    (DSA-2311-1), policykit-1 (DSA-2319-1)

* Protecting against memory recovery
  - Set more appropriate Linux VM config before wiping memory. These
    parameters should make the wipe process more robust and efficient.
```

4. On Friday, October 28th, we released Tor 0.2.2.34. Tor 0.2.2.34 fixes a critical anonymity vulnerability where an attacker can deanonymize Tor users. Everybody should upgrade.

   The attack relies on four components: 1) Clients reuse their TLS cert when talking to different relays, so relays can recognize a user by the identity key in her cert. 2) An attacker who knows the client's identity key can probe each guard relay to see if that identity key is connected

to that guard relay right now. 3) A variety of active attacks in the literature (starting from "Low-Cost Traffic Analysis of Tor" by Murdoch and Danezis in 2005) allow a malicious website to discover the guard relays that a Tor user visiting the website is using. 4) Clients typically pick three guards at random, so the set of guards for a given user could well be a unique fingerprint for her. This release fixes components 1 and 2, which is enough to block the attack; the other two remain as open research problems.

Special thanks to "frosty_un" for reporting the issue to us! (As far as we know, this has nothing to do with any claimed attack currently getting attention in the media.)

Clients should upgrade so they are no longer recognizable by the TLS certs they present. Relays should upgrade so they no longer allow a remote attacker to probe them to test whether unpatched clients are currently connected to them.

This release also fixes several vulnerabilities that allow an attacker to enumerate bridge relays. Some bridge enumeration attacks still remain; see for example proposal 188.

Changes in version 0.2.2.34 - 2011-10-26

```
o Privacy/anonymity fixes (clients):
  - Clients and bridges no longer send TLS certificate chains on
    outgoing OR connections. Previously, each client or bridge would
    use the same cert chain for all outgoing OR connections until
    its IP address changes, which allowed any relay that the client
    or bridge contacted to determine which entry guards it is using.
    Fixes CVE-2011-2768. Bugfix on 0.0.9pre5; found by "frosty_un".
  - If a relay receives a CREATE_FAST cell on a TLS connection, it
    no longer considers that connection as suitable for satisfying a
    circuit EXTEND request. Now relays can protect clients from the
    CVE-2011-2768 issue even if the clients haven't upgraded yet.
  - Directory authorities no longer assign the Guard flag to relays
    that haven't upgraded to the above "refuse EXTEND requests
    to client connections" fix. Now directory authorities can
    protect clients from the CVE-2011-2768 issue even if neither
    the clients nor the relays have upgraded yet. There's a new
    "GiveGuardFlagTo_CVE_2011_2768_VulnerableRelays" config option
    to let us transition smoothly, else tomorrow there would be no
    guard relays.

o Privacy/anonymity fixes (bridge enumeration):
  - Bridge relays now do their directory fetches inside Tor TLS
    connections, like all the other clients do, rather than connecting
    directly to the DirPort like public relays do. Removes another
    avenue for enumerating bridges. Fixes bug 4115; bugfix on 0.2.0.35.
  - Bridges relays now build circuits for themselves in a more similar
    way to how clients build them. Removes another avenue for
    enumerating bridges. Fixes bug 4124; bugfix on 0.2.0.3-alpha,
    when bridges were introduced.
```

- Bridges now refuse CREATE or CREATE_FAST cells on OR connections that they initiated. Relays could distinguish incoming bridge connections from client connections, creating another avenue for enumerating bridges. Fixes CVE-2011-2769. Bugfix on 0.2.0.3-alpha. Found by "frosty_un".

o Major bugfixes:
- Fix a crash bug when changing node restrictions while a DNS lookup is in-progress. Fixes bug 4259; bugfix on 0.2.2.25-alpha. Bugfix by "Tey'".
- Don't launch a useless circuit after failing to use one of a hidden service's introduction points. Previously, we would launch a new introduction circuit, but not set the hidden service which that circuit was intended to connect to, so it would never actually be used. A different piece of code would then create a new introduction circuit correctly. Bug reported by katmagic and found by Sebastian Hahn. Bugfix on 0.2.1.13-alpha; fixes bug 4212.

o Minor bugfixes:
- Change an integer overflow check in the OpenBSD_Malloc code so that GCC is less likely to eliminate it as impossible. Patch from Mansour Moufid. Fixes bug 4059.
- When a hidden service turns an extra service-side introduction circuit into a general-purpose circuit, free the rend_data and intro_key fields first, so we won't leak memory if the circuit is cannibalized for use as another service-side introduction circuit. Bugfix on 0.2.1.7-alpha; fixes bug 4251.
- Bridges now skip DNS self-tests, to act a little more stealthily. Fixes bug 4201; bugfix on 0.2.0.3-alpha, which first introduced bridges. Patch by "warms0x".
- Fix internal bug-checking logic that was supposed to catch failures in digest generation so that it will fail more robustly if we ask for a nonexistent algorithm. Found by Coverity Scan. Bugfix on 0.2.2.1-alpha; fixes Coverity CID 479.
- Report any failure in init_keys() calls launched because our IP address has changed. Spotted by Coverity Scan. Bugfix on 0.1.1.4-alpha; fixes CID 484.

o Minor bugfixes (log messages and documentation):
- Remove a confusing dollar sign from the example fingerprint in the man page, and also make the example fingerprint a valid one. Fixes bug 4309; bugfix on 0.2.1.3-alpha.
- The next version of Windows will be called Windows 8, and it has a major version of 6, minor version of 2. Correctly identify that version instead of calling it "Very recent version". Resolves

```
    ticket 4153; reported by funkstar.
  - Downgrade log messages about circuit timeout calibration from
    "notice" to "info": they don't require or suggest any human
    intervention. Patch from Tom Lowenthal. Fixes bug 4063;
    bugfix on 0.2.2.14-alpha.

o Minor features:
  - Turn on directory request statistics by default and include them in
    extra-info descriptors. Don't break if we have no GeoIP database.
    Backported from 0.2.3.1-alpha; implements ticket 3951.
  - Update to the October 4 2011 Maxmind GeoLite Country database.
```

5. On Friday October 28th, we released Tor 0.2.3.6-alpha. Tor 0.2.3.6-alpha includes the fix from 0.2.2.34 for a critical anonymity vulnerability where an attacker can deanonymize Tor users: `https://lists.torproject.org/pipermail/tor-announce/2011-October/000082.html`.

   Everybody should upgrade.

   This release also features support for a new v3 connection handshake protocol, and fixes to make hidden service connections more robust.

   Changes in version 0.2.3.6-alpha - 2011-10-26

```
o Major features:
  - Implement a new handshake protocol (v3) for authenticating Tors to
    each other over TLS. It should be more resistant to fingerprinting
    than previous protocols, and should require less TLS hacking for
    future Tor implementations. Implements proposal 185.
  - Allow variable-length padding cells to disguise the length of
    Tor's TLS records. Implements part of proposal 184.

o Privacy/anonymity fixes (clients):
  - Clients and bridges no longer send TLS certificate chains on
    outgoing OR connections. Previously, each client or bridge would
    use the same cert chain for all outgoing OR connections until
    its IP address changes, which allowed any relay that the client
    or bridge contacted to determine which entry guards it is using.
    Fixes CVE-2011-2768. Bugfix on 0.0.9pre5; found by "frosty_un".
  - If a relay receives a CREATE_FAST cell on a TLS connection, it
    no longer considers that connection as suitable for satisfying a
    circuit EXTEND request. Now relays can protect clients from the
    CVE-2011-2768 issue even if the clients haven't upgraded yet.
  - Directory authorities no longer assign the Guard flag to relays
    that haven't upgraded to the above "refuse EXTEND requests
    to client connections" fix. Now directory authorities can
    protect clients from the CVE-2011-2768 issue even if neither
    the clients nor the relays have upgraded yet. There's a new
    "GiveGuardFlagTo_CVE_2011_2768_VulnerableRelays" config option
```

to let us transition smoothly, else tomorrow there would be no guard relays.

o Major bugfixes (hidden services):
- Improve hidden service robustness: when an attempt to connect to a hidden service ends, be willing to refetch its hidden service descriptors from each of the HSDir relays responsible for them immediately. Previously, we would not consider refetching the service's descriptors from each HSDir for 15 minutes after the last fetch, which was inconvenient if the hidden service was not running during the first attempt. Bugfix on 0.2.0.18-alpha; fixes bug 3335.
- When one of a hidden service's introduction points appears to be unreachable, stop trying it. Previously, we would keep trying to build circuits to the introduction point until we lost the descriptor, usually because the user gave up and restarted Tor. Partly fixes bug 3825.
- Don't launch a useless circuit after failing to use one of a hidden service's introduction points. Previously, we would launch a new introduction circuit, but not set the hidden service which that circuit was intended to connect to, so it would never actually be used. A different piece of code would then create a new introduction circuit correctly. Bug reported by katmagic and found by Sebastian Hahn. Bugfix on 0.2.1.13-alpha; fixes bug 4212.

o Major bugfixes (other):
- Bridges now refuse CREATE or CREATE_FAST cells on OR connections that they initiated. Relays could distinguish incoming bridge connections from client connections, creating another avenue for enumerating bridges. Fixes CVE-2011-2769. Bugfix on 0.2.0.3-alpha. Found by "frosty_un".
- Don't update the AccountingSoftLimitHitAt state file entry whenever tor gets started. This prevents a wrong average bandwidth estimate, which would cause relays to always start a new accounting interval at the earliest possible moment. Fixes bug 2003; bugfix on 0.2.2.7-alpha. Reported by BryonEldridge, who also helped immensely in tracking this bug down.
- Fix a crash bug when changing node restrictions while a DNS lookup is in-progress. Fixes bug 4259; bugfix on 0.2.2.25-alpha. Bugfix by "Tey'".

o Minor bugfixes (on 0.2.2.x and earlier):
- When a hidden service turns an extra service-side introduction circuit into a general-purpose circuit, free the rend_data and intro_key fields first, so we won't leak memory if the circuit is cannibalized for use as another service-side introduction

circuit. Bugfix on 0.2.1.7-alpha; fixes bug 4251.
- Rephrase the log message emitted if the TestSocks check is successful. Patch from Fabian Keil; fixes bug 4094.
- Bridges now skip DNS self-tests, to act a little more stealthily. Fixes bug 4201; bugfix on 0.2.0.3-alpha, which first introduced bridges. Patch by "warms0x".
- Remove a confusing dollar sign from the example fingerprint in the man page, and also make the example fingerprint a valid one. Fixes bug 4309; bugfix on 0.2.1.3-alpha.
- Fix internal bug-checking logic that was supposed to catch failures in digest generation so that it will fail more robustly if we ask for a nonexistent algorithm. Found by Coverity Scan. Bugfix on 0.2.2.1-alpha; fixes Coverity CID 479.
- Report any failure in init_keys() calls launched because our IP address has changed. Spotted by Coverity Scan. Bugfix on 0.1.1.4-alpha; fixes CID 484.

o Minor bugfixes (on 0.2.3.x):
- Fix a bug in configure.in that kept it from building a configure script with autoconf versions earlier than 2.61. Fixes bug 2430; bugfix on 0.2.3.1-alpha.
- Don't warn users that they are exposing a client port to the Internet if they have specified an RFC1918 address. Previously, we would warn if the user had specified any non-loopback address. Bugfix on 0.2.3.3-alpha. Fixes bug 4018; reported by Tas.
- Fix memory leaks in the failing cases of the new SocksPort and ControlPort code. Found by Coverity Scan. Bugfix on 0.2.3.3-alpha; fixes coverity CIDs 485, 486, and 487.

o Minor features:
- When a hidden service's introduction point times out, consider trying it again during the next attempt to connect to the HS. Previously, we would not try it again unless a newly fetched descriptor contained it. Required by fixes for bugs 1297 and 3825.
- The next version of Windows will be called Windows 8, and it has a major version of 6, minor version of 2. Correctly identify that version instead of calling it "Very recent version". Resolves ticket 4153; reported by funkstar.
- The Bridge Authority now writes statistics on how many bridge descriptors it gave out in total, and how many unique descriptors it gave out. It also lists how often the most and least commonly fetched descriptors were given out, as well as the median and 25th/75th percentile. Implements tickets 4200 and 4294.
- Update to the October 4 2011 Maxmind GeoLite Country database.

```
  o Code simplifications and refactoring:
    - Remove some old code to remember statistics about which descriptors
      we've served as a directory mirror. The feature wasn't used and
      is outdated now that microdescriptors are around.
    - Rename Tor functions that turn strings into addresses, so that
      "parse" indicates that no hostname resolution occurs, and
      "lookup" indicates that hostname resolution may occur. This
      should help prevent mistakes in the future. Fixes bug 3512.
```

6. On October 30th, we released Tor 0.2.3.7-alpha. Tor 0.2.3.7-alpha fixes a crash bug in 0.2.3.6-alpha introduced by the new v3 handshake. It also resolves yet another bridge address enumeration issue.

```
Changes in version 0.2.3.7-alpha - 2011-10-30
  o Major bugfixes:
    - If we mark an OR connection for close based on a cell we process,
      don't process any further cells on it. We already avoid further
      reads on marked-for-close connections, but now we also discard the
      cells we'd already read. Fixes bug 4299; bugfix on 0.2.0.10-alpha,
      which was the first version where we might mark a connection for
      close based on processing a cell on it.
    - Fix a double-free bug that would occur when we received an invalid
      certificate in a CERT cell in the new v3 handshake. Fixes bug 4343;
      bugfix on 0.2.3.6-alpha.
    - Bridges no longer include their address in NETINFO cells on outgoing
      OR connections, to allow them to blend in better with clients.
      Removes another avenue for enumerating bridges. Reported by
      "troll_un". Fixes bug 4348; bugfix on 0.2.0.10-alpha, when NETINFO
      cells were introduced.

  o Trivial fixes:
    - Fixed a typo in a hibernation-related log message. Fixes bug 4331;
      bugfix on 0.2.2.23-alpha; found by "tmpname0901".
```

Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- Developed short user manual to ship with get-tor email autoresponses, and for a single page reference guide to Tor. See `https://torproject.org/docs/short-user-manual.html.en`.
- Tor users requesting packages too large for their email provider to accept now get a nice and polite note from GetTor. Part of `https://trac.torproject.org/projects/tor/ticket/3920`, `https://trac.torproject.org/projects/tor/ticket/4166`, and `https://trac.torproject.org/projects/tor/ticket/2520`.

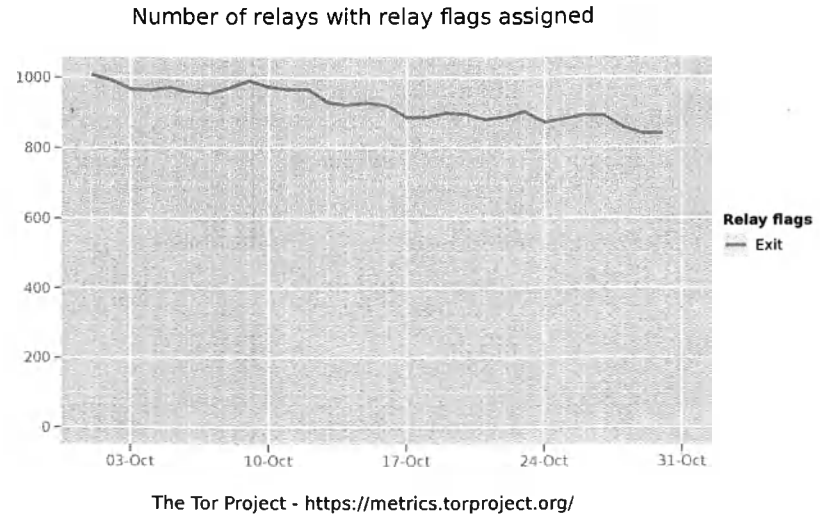
- Added GetTor package updates to cron so we don't need to run the package fetching and updating mechanism by hand.
- Added five new website and distribution mirrors, https://www.torproject.org/getinvolved/mirrors.html.en.
- Researching some new blocking mechanisms seen in China regarding Tor bridges. Tracked at https://trac.torproject.org/projects/tor/ticket/4185. Need to collect more data. Others unrelated to Tor may be seeing something similar, http://www.nsc.liu.se/~nixon/sshprobes.html.

Hide Tor's network signature.

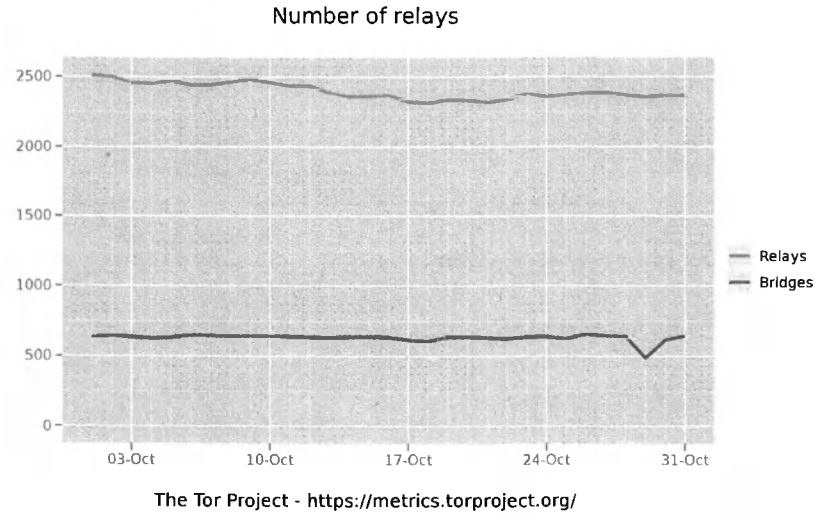
- Modular transports are a way to decouple protocol-level obfuscation from the core Tor protocol in order to better resist client-bridge censorship. Our approach is to specify a means to add pluggable transport implementations to Tor clients and bridges so that they can negotiate a superencipherment for the Tor protocol. We described the necessary changes to Tor in proposal 180, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/180-pluggable-transport.txt. The implementation is mostly done, but not merged yet, which should be done by the end of November.
- We built obfsproxy, https://gitweb.torproject.org/obfsproxy.git/blob/HEAD:/doc/protocol-spec.txt, which is a protocol obfuscation layer for TCP protocols. obfsproxy does not provide authentication or data integrity and does not hide data lengths. It is more suitable for providing a layer of obfuscation for an existing authenticated protocol, like SSH or TLS.
- Tor 0.2.3.6 is the first version to contain a new handshake protocol (v3) for authenticating Tors to each other over TLS. The v3 protocol should allow us to become more resistant to fingerprinting than previous protocols, and should require less TLS hacking for future Tor implementations. Implements proposal 176, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/176-revising-handshake.txt. The v3 protocol gets used between any two Tors that both are running Tor version 0.2.3.6 or later. There are still bugs in the v3 handshake code, the most significant of which are fixed in Tor 0.2.3.7.

Grow the Tor network and user base. Outreach.

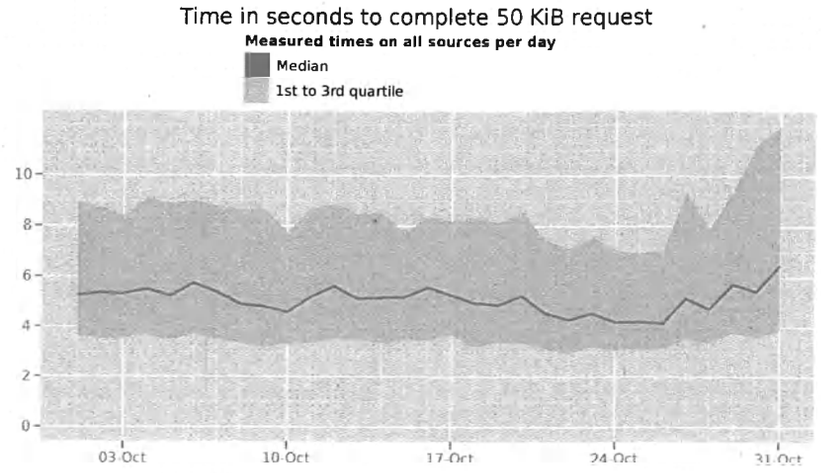
Measures of the Tor Network



This graph shows the total quantity of exit relays in October 2011. There is a reduction of 200 exit relays over the month for unknown reasons. Possibly a number of relays switched from exit to non-exit roles.

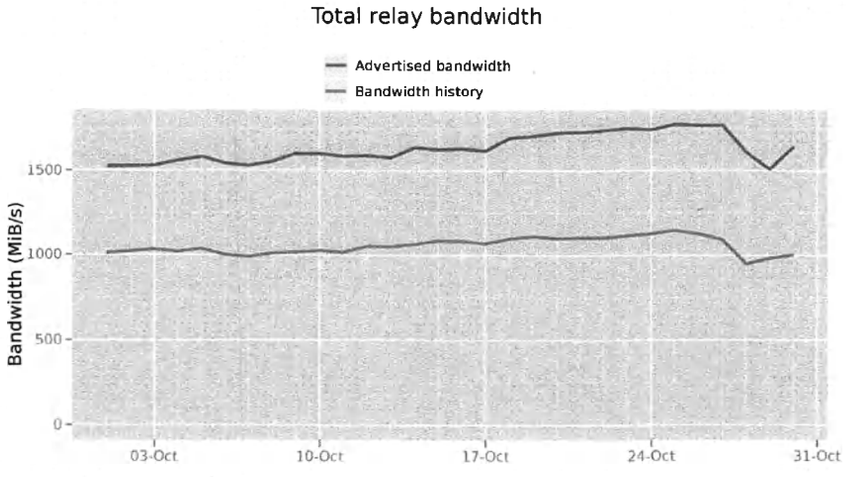


This graph shows the total quantity of relays and the total quantity of bridges in October 2011.



The Tor Project - https://metrics.torproject.org/

This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Average latency has increased slightly to 6 seconds at the end of the month. This is likely due to the loss of a number of exit relays throughout the month.



The Tor Project - https://metrics.torproject.org/

This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The decrease in relays overall reduces the available bandwidth. We're still at a capacity of 1.6 GBps (12.8 Gbps) available with 1 GBps (8 Gbps) used.

Outreach and Advocacy

1. Jacob, Roger, and Arturo traveled to Tunisia for the 2011 Arab Blogger Conference. Roger wrote up a detailed trip report at https://blog.torproject.org/blog/trip-report-arab-bloggers-mee

2. The Persian News Network did a 14 minute segment on Tor, censorship circumvention, and empowering citizens to gain access to information. A copy of the video segment is available at https://media.torproject.org/video/PERSIAN_2_0.mp4.

3. Damian represented Tor at the Google Summer of Code 2011 Mentor Summit, http://gsoc-wiki.osuosl.org/index.php/2011.

4. Karen, Runa, and Mike attended the Silicon Valley Human Rights Conference, https://www.rightscon.org/.

5. Jacob spoke at the Julia Group/Sida Internet and Democratic Change conference, http://juliagruppen.se/lang/en/2011/09/internet-och-demokratisk-forandringinternet-and-democrati

6. Andrew, Roger, Nick, and Runa produced a public response to various rumors of Tor's global compromise, https://blog.torproject.org/blog/rumors-tors-compromise-are-greatly-exaggerate

7. Jacob attended ISS World in Washington DC to learn about the current state of the art in detecting Tor, http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques Jacob was asked to leave on the second day of the conference.

8. Jacob and others found evidence that Blue Coat Systems devices are being used in Syria, furthermore to possibly track and filter Tor connections to public relays. http://motherjones.com/mojo/2011/10/blue-coat-admits-syria-connection.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- We publicly announced our intention to reconfigure our software into Tor Browser Bundle, and various relay/bridge/exit-relay by default bundles for easier client configuration and usage, https://blog.torproject.org/blog/plain-vidalia-bundles-be-discontinued-dont-panic.

- Started a draft of the Tor Browser Design, https://www.torproject.org/projects/torbrowser/design/. This document describes the adversary model, design requirements, implementation, packaging and testing procedures of the Tor Browser. It is current as of Tor Browser 2.2.33-3.

  This document is also meant to serve as a set of design requirements and to describe a reference implementation of a Private Browsing Mode that defends against active network adversaries, in addition to the passive forensic local adversary currently addressed by the major browsers.

Bridge relay and bridge authority work.

- Karsten analyzed what fraction of bridges does not report statistics (https://trac.torproject.org/projects/tor/ticket/3261). Next step will be to investigate reasons why bridges don't report statistics (less than 24 hours uptime, delayed descriptor publication, old versions, etc.).

- Karsten finished a bridge stability analysis (https://trac.torproject.org/projects/tor/ticket/4255). The focus is how BridgeDB can track bridge stability and give out at least one stable bridge per user https://metrics.torproject.org/papers/bridge-stability-2011-10-31.pdf.

Scalability, load balancing, directory overhead, efficiency.

- Setup a new bandwidth authority in Sweden. We now have five bandwidth authorities measuring and load balancing the Tor network.
- Replaced a bandwidth authority with new dedicated hardware for more reliable measurements and performance. A snowstorm promptly took out its Internet connection for two days. The authority is backonline and operating within acceptable parameters.
- Nick finished and merged his implementation of proposal 176 to provide the v3 handshake protocol. This removes the need for TLS renegotiation from the Tor handshake protocol. See https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/176-revising-handshake.txt for details.
- Nick wrote proposal 186 to describe how to give multiple ORPorts and addresses to a Tor node so as to make IPv6 migration plausible. This may be over-engineered; more discussion needed. Proposal 186 can be found at https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/186-multiple-orports.txt.
- Nick wrote proposal 187 to specify a way to allow a future cell type for a client authorization step. Proposal 187 can be found at https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/187-allow-client-auth.txt.
- Nick wrote proposal 188 to explain bridge guards, a fairly versatile (though not absolutely comprehensive) anti-enumeration mechanism. Proposal 188 can be found at https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/188-bridge-guards.txt.
- Nick wrote a long but important document explaining (ok, guessing) where we should take our crypto over the next year or so. More insight and thoughts are needed. Join the conversation at https://lists.torproject.org/pipermail/tor-dev/2011-November/002999.html.

Incentives work.

Nothing to report.

More reliable (e.g. split) download mechanism.

Nothing to report.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- Translation updates for get-tor, vidalia, vidalia-help, vidalia-installer, short user manual, bridge db, torbutton, and orbot.
- Language translation updates in Hebrew, Arabic, Catalan, Danish, German, Greek, Spanish, Persian, French, Hindi, Hungarian, Macedonian, Norwegian, Dutch, Polish, Slovenian, Serbian, Swedish, and Mandarin Chinese.
- Find all of the supported languages and their current translation status at `https://www.transifex.net/projects/p/torproject/r/all-resources/`.

October 17, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our 41st invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at [redacted] if there are any questions.

Invoice 41:

Period	Months	Rate	Cost
08/17/2011 - 09/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG10172011

From: Andrew Lewman, Executive Director
To: The Tor Community
Date: October 7, 2011

This report documents progress in September 2011.

New releases, new hires, new funding

New Funding

Tor receives funding from the Swedish International Cooperation Development Agency to improve the Tails live system.

New Releases

1. On September 1st, we released Tor 0.2.3.3-alpha. Tor 0.2.3.3-alpha adds a new "stream isolation" feature to improve Tor's security, and provides client-side support for the microdescriptor and optimistic data features introduced earlier in the 0.2.3.x series. It also includes numerous critical bugfixes in the (optional) bufferevent-based networking backend.

```
Changes in version 0.2.3.3-alpha - 2011-09-01
  o Major features (stream isolation):
    - You can now configure Tor so that streams from different
      applications are isolated on different circuits, to prevent an
      attacker who sees your streams as they leave an exit node from
      linking your sessions to one another. To do this, choose some way
      to distinguish the applications: have them connect to different
      SocksPorts, or have one of them use SOCKS4 while the other uses
      SOCKS5, or have them pass different authentication strings to the
      SOCKS proxy. Then, use the new SocksPort syntax to configure the
      degree of isolation you need. This implements Proposal 171.
    - There's a new syntax for specifying multiple client ports (such as
      SOCKSPort, TransPort, DNSPort, NATDPort): you can now just declare
      multiple *Port entries with full addr:port syntax on each.
      The old *ListenAddress format is still supported, but you can't
      mix it with the new *Port syntax.

  o Major features (other):
    - Enable microdescriptor fetching by default for clients. This allows
      clients to download a much smaller amount of directory information.
```

```
    To disable it (and go back to the old-style consensus and
    descriptors), set "UseMicrodescriptors 0" in your torrc file.
  - Tor's firewall-helper feature, introduced in 0.2.3.1-alpha (see the
    "PortForwarding" config option), now supports Windows.
  - When using an exit relay running 0.2.3.x, clients can now
    "optimistically" send data before the exit relay reports that
    the stream has opened. This saves a round trip when starting
    connections where the client speaks first (such as web browsing).
    This behavior is controlled by a consensus parameter (currently
    disabled). To turn it on or off manually, use the "OptimisticData"
    torrc option. Implements proposal 181; code by Ian Goldberg.

o Major bugfixes (bufferevents, fixes on 0.2.3.1-alpha):
  - When using IOCP on Windows, we need to enable Libevent windows
    threading support.
  - The IOCP backend now works even when the user has not specified
    the (internal, debugging-only) _UseFilteringSSLBufferevents option.
    Fixes part of bug 3752.
  - Correctly record the bytes we've read and written when using
    bufferevents, so that we can include them in our bandwidth history
    and advertised bandwidth. Fixes bug 3803.
  - Apply rate-limiting only at the bottom of a chain of filtering
    bufferevents. This prevents us from filling up internal read
    buffers and violating rate-limits when filtering bufferevents
    are enabled. Fixes part of bug 3804.
  - Add high-watermarks to the output buffers for filtered
    bufferevents. This prevents us from filling up internal write
    buffers and wasting CPU cycles when filtering bufferevents are
    enabled. Fixes part of bug 3804.
  - Correctly notice when data has been written from a bufferevent
    without flushing it completely. Fixes bug 3805.
  - Fix a bug where server-side tunneled bufferevent-based directory
    streams would get closed prematurely. Fixes bug 3814.
  - Fix a use-after-free error with per-connection rate-limiting
    buckets. Fixes bug 3888.

o Major bugfixes (also part of 0.2.2.31-rc):
  - If we're configured to write our ControlPorts to disk, only write
    them after switching UID and creating the data directory. This way,
    we don't fail when starting up with a nonexistent DataDirectory
    and a ControlPortWriteToFile setting based on that directory. Fixes
    bug 3747; bugfix on Tor 0.2.2.26-beta.

o Minor features:
  - Added a new CONF_CHANGED event so that controllers can be notified
```

of any configuration changes made by other controllers, or by the user. Implements ticket 1692.
- Use evbuffer_copyout() in inspect_evbuffer(). This fixes a memory leak when using bufferevents, and lets Libevent worry about how to best copy data out of a buffer.
- Replace files in stats/ rather than appending to them. Now that we include statistics in extra-info descriptors, it makes no sense to keep old statistics forever. Implements ticket 2930.

o Minor features (build compatibility):
- Limited, experimental support for building with nmake and MSVC.
- Provide a substitute implementation of lround() for MSVC, which apparently lacks it. Patch from Gisle Vanem.

o Minor features (also part of 0.2.2.31-rc):
- Update to the August 2 2011 Maxmind GeoLite Country database.

o Minor bugfixes (on 0.2.3.x-alpha):
- Fix a spurious warning when parsing SOCKS requests with bufferevents enabled. Fixes bug 3615; bugfix on 0.2.3.2-alpha.
- Get rid of a harmless warning that could happen on relays running with bufferevents. The warning was caused by someone doing an http request to a relay's orport. Also don't warn for a few related non-errors. Fixes bug 3700; bugfix on 0.2.3.1-alpha.

o Minor bugfixes (on 2.2.x and earlier):
- Correct the man page to explain that HashedControlPassword and CookieAuthentication can both be set, in which case either method is sufficient to authenticate to Tor. Bugfix on 0.2.0.7-alpha, when we decided to allow these config options to both be set. Issue raised by bug 3898.
- The "--quiet" and "--hush" options now apply not only to Tor's behavior before logs are configured, but also to Tor's behavior in the absense of configured logs. Fixes bug 3550; bugfix on 0.2.0.10-alpha.

o Minor bugfixes (also part of 0.2.2.31-rc):
- Write several files in text mode, on OSes that distinguish text mode from binary mode (namely, Windows). These files are: 'buffer-stats', 'dirreq-stats', and 'entry-stats' on relays that collect those statistics; 'client_keys' and 'hostname' for hidden services that use authentication; and (in the tor-gencert utility) newly generated identity and signing keys. Previously, we wouldn't specify text mode or binary mode, leading to an assertion failure. Fixes bug 3607. Bugfix on 0.2.1.1-alpha (when

```
    the DirRecordUsageByCountry option which would have triggered
    the assertion failure was added), although this assertion failure
    would have occurred in tor-gencert on Windows in 0.2.0.1-alpha.
  - Selectively disable deprecation warnings on OS X because Lion
    started deprecating the shipped copy of openssl. Fixes bug 3643.
  - Remove an extra pair of quotation marks around the error
    message in control-port STATUS_GENERAL BUG events. Bugfix on
    0.1.2.6-alpha; fixes bug 3732.
  - When unable to format an address as a string, report its value
    as "???" rather than reusing the last formatted address. Bugfix
    on 0.2.1.5-alpha.

o Code simplifications and refactoring:
  - Rewrite the listener-selection logic so that parsing which ports
    we want to listen on is now separate from binding to the ports
    we want.

o Build changes:
  - Building Tor with bufferevent support now requires Libevent
    2.0.13-stable or later. Previous versions of Libevent had bugs in
    SSL-related bufferevents and related issues that would make Tor
    work badly with bufferevents. Requiring 2.0.13-stable also allows
    Tor with bufferevents to take advantage of Libevent APIs
    introduced after 2.0.8-rc.
```

2. On September 10th, we released new Tor Browser Bundles.

```
Important note to Windows users: in the last release we enabled automatic
port selection for Tor and this had very unexpected side effects on
many Windows machines. It turns out that there are a number of consumer
firewalls that don't like things connecting on high ports, which was the
default. We're looking into smarter ways to handle this failure mode,
but until we find one, we have reverted the behavior to using the previous
static port. We're very sorry for the huge inconvenience this caused and
hope you will find these bundles more bug-free!

Tor Browser Bundle (2.2.32-4)

    Windows fixes

        Disable automatic port selection to accommodate Windows users
        with firewalls that don't allow connections or traffic on high
        ports (closes: #3952, #3945)

    Linux fixes
        Fix Makefile to allow for automatic retrieval of Qt and libpng
```

```
    (closes: #2255)
    Remove symlinks from tarball (closes: #2312)

  General fixes and updates
    New Firefox patches
      Prevent Firefox from loading all system plugins besides Flash
      (closes: #2826, #3547)
      Prevent content-preferences service from writing website
      urls and their settings to disk (closes: #3229)
    Update Torbutton to 1.4.3
      Don't let Torbutton inadvertently enable automatic updating
      in Firefox (closes: #3933)
      Fix auto-scroll on Twitter (closes: #3960)
      Allow site zoom information to be stored (closes: #3928)
      Make permissions and disk errors human-readable (closes: #3649)
```

3. On September 13th we released Tor 0.2.3.4-alpha. Tor 0.2.3.4-alpha includes the fixes from 0.2.2.33, including a slight tweak to Tor's TLS handshake that makes relays and bridges that run this new version reachable from Iran again. It also fixes a few new bugs in 0.2.3.x, and teaches relays to recognize when they're not listed in the network consensus and republish.

```
Changes in version 0.2.3.4-alpha - 2011-09-13
  o Major bugfixes (also part of 0.2.2.33):
    - Avoid an assertion failure when reloading a configuration with
      TrackExitHosts changes. Found and fixed by 'laruldan'. Fixes bug
      3923; bugfix on 0.2.2.25-alpha.

  o Minor features (security, also part of 0.2.2.33):
    - Check for replays of the public-key encrypted portion of an
      INTRODUCE1 cell, in addition to the current check for replays of
      the g^x value. This prevents a possible class of active attacks
      by an attacker who controls both an introduction point and a
      rendezvous point, and who uses the malleability of AES-CTR to
      alter the encrypted g^x portion of the INTRODUCE1 cell. We think
      that these attacks is infeasible (requiring the attacker to send
      on the order of zettabytes of altered cells in a short interval),
      but we'd rather block them off in case there are any classes of
      this attack that we missed. Reported by Willem Pinckaers.

  o Minor features (also part of 0.2.2.33):
    - Adjust the expiration time on our SSL session certificates to
      better match SSL certs seen in the wild. Resolves ticket 4014.
    - Change the default required uptime for a relay to be accepted as
      a HSDir (hidden service directory) from 24 hours to 25 hours.
      Improves on 0.2.0.10-alpha; resolves ticket 2649.
    - Add a VoteOnHidServDirectoriesV2 config option to allow directory
```

authorities to abstain from voting on assignment of the HSDir consensus flag. Related to bug 2649.
- Update to the September 6 2011 Maxmind GeoLite Country database.

o Minor bugfixes (also part of 0.2.2.33):
- Demote the 'replay detected' log message emitted when a hidden service receives the same Diffie-Hellman public key in two different INTRODUCE2 cells to info level. A normal Tor client can cause that log message during its normal operation. Bugfix on 0.2.1.6-alpha; fixes part of bug 2442.
- Demote the 'INTRODUCE2 cell is too {old,new}' log message to info level. There is nothing that a hidden service's operator can do to fix its clients' clocks. Bugfix on 0.2.1.6-alpha; fixes part of bug 2442.
- Clarify a log message specifying the characters permitted in HiddenServiceAuthorizeClient client names. Previously, the log message said that "[A-Za-z0-9+-_]" were permitted; that could have given the impression that every ASCII character between "+" and "_" was permitted. Now we say "[A-Za-z0-9+_-]". Bugfix on 0.2.1.5-alpha.

o Build fixes (also part of 0.2.2.33):
- Clean up some code issues that prevented Tor from building on older BSDs. Fixes bug 3894; reported by "grarpamp".
- Search for a platform-specific version of "ar" when cross-compiling. Should fix builds on iOS. Resolves bug 3909, found by Marco Bonetti.

o Major bugfixes:
- Fix a bug where the SocksPort option (for example) would get ignored and replaced by the default if a SocksListenAddress option was set. Bugfix on 0.2.3.3-alpha; fixes bug 3936. Fix by Fabian Keil.

o Major features:
- Relays now try regenerating and uploading their descriptor more frequently if they are not listed in the consensus, or if the version of their descriptor listed in the consensus is too old. This fix should prevent situations where a server declines to re-publish itself because it has done so too recently, even though the authorities decided not to list its recent-enough descriptor. Fix for bug 3327.

o Minor features:
- Relays now include a reason for regenerating their descriptors in an HTTP header when uploading to the authorities. This will make it easier to debug descriptor-upload issues in the future.

```
    - When starting as root and then changing our UID via the User
      control option, and we have a ControlSocket configured, make sure
      that the ControlSocket is owned by the same account that Tor will
      run under. Implements ticket 3421; fix by Jérémy Bobbio.

  o Minor bugfixes:
    - Abort if tor_vasprintf fails in connection_printf_to_buf (a
      utility function used in the control-port code). This shouldn't
      ever happen unless Tor is completely out of memory, but if it did
      happen and Tor somehow recovered from it, Tor could have sent a log
      message to a control port in the middle of a reply to a controller
      command. Fixes part of bug 3428; bugfix on 0.1.2.3-alpha.
    - Make 'FetchUselessDescriptors' cause all descriptor types and
      all consensus types (including microdescriptors) to get fetched.
      Fixes bug 3851; bugfix on 0.2.3.1-alpha.

  o Code refactoring:
    - Make a new "entry connection" struct as an internal subtype of "edge
      connection", to simplify the code and make exit connections smaller.
```

4. On September 21st, an updated version of the Tails Anonymous Live System was released. Major changes include an update to the base operating system, switch to the new Tor stable branch, Torbutton update, and better nickname randomization inside Pidgin.

   A detailed changelog is below:

```
  * Rebase on the Debian Squeeze 6.0.2.1 point-release.

  * Tor
    - Update to 0.2.2.33-1.
    - Disabled ControlPort in favour of ControlSocket.
    - Add port 6523 (Gobby) to Tor's LongLivedPorts list.

  * I2P
    - Update to 0.8.8.
    - Start script now depends on HTP since I2P breaks if the clock jumps or is
      too skewed during bootstrap.

  * Iceweasel
    - Update to 3.5.16-9 (fixes CVE-2011-2374, CVE-2011-2376, CVE-2011-2365,
      CVE-2011-2373, CVE-2011-2371, CVE-2011-0083, CVE-2011-2363, CVE-2011-0085,
      CVE-2011-2362, CVE-2011-2982, CVE-2011-2981, CVE-2011-2378, CVE-2011-2984,
      CVE-2011-2983).
    - Enable HTTP pipelining (like TBB).
    - Update HTTPS Everywhere extension to 1.0.1-1 from Debian unstable.
    - Suppress FoxyProxy update prompts.
```

  - Prevent FoxyProxy from "phoning home" after a detected upgrade.
  - Fixed a bunch of buggy regular expressions in FoxyProxy's configuration. See [[bugs/exploitable_typo_in_url_regex?]] for details. Note that none of these issues are critical due to the transparent proxy.
  - Add DuckDuckGo SSL search engine.

* Torbutton
  - Update to torbutton 1.4.3-1 from Debian unstable.
  - Don't show Torbutton status in the status bar as it's now displayed in the toolbar instead.

* Pidgin
  - More random looking nicks in pidgin.
  - Add IRC account on chat.wikileaks.de:9999.

* HTP
  - Upgrade htpdate script (taken from Git 7797fe9) that allows setting wget's --dns-timeout option.

* Software
  - Update Linux to 3.0.0-1. -686 is now deprecated in favour of -486 and -686-pae; the world is not ready for -pae yet, so we now ship -486.
  - Update OpenSSL to 0.9.8o-4squeeze2 (fixes CVE-2011-1945 (revoke compromised DigiNotar certificates), CVE-2011-1945).
  - Update Vidalia to 0.2.14-1+tails1 custom package.
  - Install accessibility tools:
    - gnome-mag: screen magnifier
    - gnome-orca: text-to-speech
  - Replace the onBoard virtual keyboard with Florence.
  - Install the PiTIVi non-linear audio/video editor.
  - Install ttdnsd.
  - Install tor-arm.
  - Install lzma.

* Arbitrary DNS queries
  - Tor can not handle all types of DNS queries, so if the Tor resolver fails we fallback to ttdnsd. This is now possible with Tor 0.2.2.x, since we fixed Tor bug #3369.

* Hardware support
  - Install ipheth-utils for iPhone tethering.
  - Install xserver-xorg-input-vmmouse (for mouse integration with the host OS in VMWare and KVM).
  - Install virtualbox-ose 4.x guest packages from Debian backports.

```
  * Miscellaneous
    - Switch gpg to use keys.indymedia.org's hidden service, without SSL.
      The keys.indymedia.org SSL certificate is now self-signed. The hidden
      service gives a good enough way to authenticate the server and encrypts
      the connection, and just removes the certificates management issue.
    - The squashfs is now compressed using XZ which reduces the image size quite
      drastically.
    - Remove Windows autorun.bat and autorun.inf. These files did open a static
      copy of our website, which is not accessible any longer.

  * Build system
    - Use the Git branch instead of the Debian version into the built image's
      filename.
    - Allow replacing efficient XZ compression with quicker gzip.
    - Build and install documentation into the chroot (-> filesystem.squashfs).
      Rationale: our static website cannot be copied to a FAT32 filesystem due
      to filenames being too long. This means the documentation cannot be
      browsed offline from outside Tails. However, our installer creates GPT
      hidden partitions, so the doc would not be browseable from outside Tails
      anyway. The only usecase we really break by doing so is browsing the
      documentation while running a non-Tails system, from a Tails CD.
```

5. On September 25th, the latest Arm was released. A new release of arm (http://www.atagar.com/arm/) is now available. Besides the normal batch of bug fixes and minor features this includes an interactive interpretor for raw control port access...

   ```
   http://www.atagar.com/arm/images/screenshot_interpretor_full.png

   http://www.atagar.com/arm/releaseNotes.php#1.4.4

   This is intended to be a tool for developers, highly knowledgeable
   operators, and anyone that would like to learn about Tor's control
   protocol. It provides usability improvements like tab completion and
   history scroll-back, along with IRC style interpretor commands...

   * /help - provides usage information for all of the tor/interpretor
   commands and tor's configuration options
   * /info - queries relay information via fingerprint, nickname, or IP
   * address
   * /find - searches the backlog for the given regex
   * /events - displays any events that we've listened for
   * /write - dumps the interpretor backlog to a file

   This can both be used via a new page in the curses interface and as a
   standalone prompt by running "arm --prompt"...
   ```

6. On September 28th, we released Tor 0.2.3.5-alpha. Tor 0.2.3.5-alpha fixes two bugs that make it possible to enumerate bridge relays; fixes an assertion error that many users started hitting

today; and adds the ability to refill token buckets more often than once per second, allowing significant performance improvements.

```
Changes in version 0.2.3.5-alpha - 2011-09-28
  o Security fixes:
    - Bridge relays now do their directory fetches inside Tor TLS
      connections, like all the other clients do, rather than connecting
      directly to the DirPort like public relays do. Removes another
      avenue for enumerating bridges. Fixes bug 4115; bugfix on 0.2.0.35.
    - Bridges relays now build circuits for themselves in a more similar
      way to how clients build them. Removes another avenue for
      enumerating bridges. Fixes bug 4124; bugfix on 0.2.0.3-alpha,
      when bridges were introduced.

  o Major bugfixes:
    - Fix an "Assertion md->held_by_node == 1 failed" error that could
      occur when the same microdescriptor was referenced by two node_t
      objects at once. Fix for bug 4118; bugfix on Tor 0.2.3.1-alpha.

  o Major features (networking):
    - Add a new TokenBucketRefillInterval option to refill token buckets
      more frequently than once per second. This should improve network
      performance, alleviate queueing problems, and make traffic less
      bursty. Implements proposal 183; closes ticket 3630. Design by
      Florian Tschorsch and Björn Scheuermann; implementation by
      Florian Tschorsch.

  o Minor bugfixes:
    - Change an integer overflow check in the OpenBSD_Malloc code so
      that GCC is less likely to eliminate it as impossible. Patch
      from Mansour Moufid. Fixes bug 4059.

  o Minor bugfixes (usability):
    - Downgrade log messages about circuit timeout calibration from
      "notice" to "info": they don't require or suggest any human
      intervention. Patch from Tom Lowenthal. Fixes bug 4063;
      bugfix on 0.2.2.14-alpha.

  o Minor features (diagnostics):
    - When the system call to create a listener socket fails, log the
      error message explaining why. This may help diagnose bug 4027.
```

7. On September 30th, we released update Tor Browser Bundles which include Firefox 7.0.1 and Tor 0.2.2.33.

   ```
   The bundles were originally uploaded with Firefox 7.0, but a fix was
   ```

```
quickly released, so the two changelogs have been merged in this post.

Tor Browser Bundle (2.2.33-2)

Windows fixes

    Begin building Vidalia with DEP/ASLR

OS X fixes

    Stop TBB from logging so much information to the system by only
    allowing dyld log library loads to syslog when it is in debug mode
    (closes: #4093)

General fixes and updates

    Update Firefox to 7.0.1
    Update OpenSSL to 1.0.0e (closes: #3996) (except for OS X)
    Update Tor to 0.2.2.33
    Update NoScript to 2.1.2.8
    Downgrade HTTPS Everywhere to 1.0.3, because we don't want stable
    TBBs to use development versions of extensions (closes: #4050)
```

Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- Karsten helped Christian fix BridgeDB that depended on a working exit list which we didn't have for a week or two. Helped fix GetTor statistics together with Christian and changed the graph parameter on metrics-web from 'bundle' to 'language'.
- George from Microsoft Research came up with a second model for a censorship detector that we need to look at and maybe deploy as a second beta on the metrics website. `https://lists.torproject.org/pipermail/tor-dev/2011-September/002923.html`
- Nick spent about a day evaluating Rizzo and Duong's sexy new SSL attack, BEAST, and writing a blog post about my findings, `https://blog.torproject.org/blog/tor-and-beast-ssl-attack`
- Tomas made some progress on Vidalia:
  - Backported the ServerPage new layout to the stable branch.
  - Improved Vidalia's authentication to Tor, so that it tries CookieAuth, and HashedAuth afterwards if the former fails.
  - Merged several branches that were for review for a while, although I didn't have any reviews.

- Put tarballs for 0.2.15-rc and 0.3.1-rc in two tickets to get some testing before the actual release, so that we don't have those quick releases because I didn't catch a particular bug.
- Started doing changes files, otherwise it's really hard to keep track of everything.

- Tomas worked on Thandy. Improved the Thp package implementation so that it's almost ready for a nice interface with Vidalia or whatever controller that uses it.

- Mike wrote up our analysis and deployed a patch for website fingerprinting. Website fingerprinting is the act of recognizing web traffic through surveillance despite the use of encryption or anonymizing software. The general idea is to leverage the fact that many web sites have specific fixed request patterns and response byte counts that are known beforehand. This information can be used to recognize your web traffic despite attempts at encryption or tunneling. Websites that have an abundance of static content and a fixed request structure tend to be vulnerable to this type of surveillance. Unfortunately, there is enough static content on most websites for this to be the case.

  The full post can be read at `https://blog.torproject.org/blog/experimental-defense-website-traff`

Hide Tor's network signature.

- Nick implemented proposal 176 – the 'new handshake' one that is supposed to make our protocol a little harder to fingerprint and make it require a little less in the way of crazy SSL hacking. It's going to take a little more poking to make it as good as I'd like, and it DEFINITELY needs more review, but at the moment it seems to work for me. `https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/176-revising-handshake.txt`

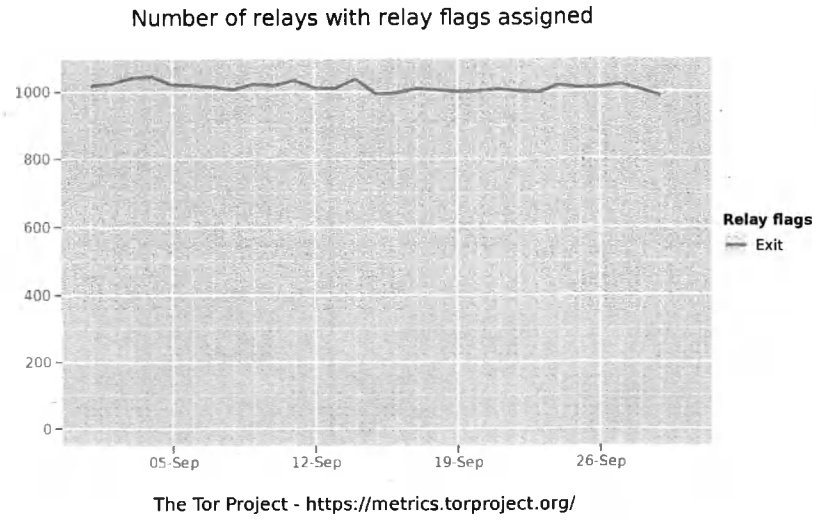
- On September 13th, Iran added a filter rule to their border routers that recognized Tor traffic and blocked it. Thanks to help from a variety of friends around the world, we quickly discovered how they were blocking it and released a new version of Tor that isn't blocked. Fortunately, the fix is on the relay side: that means once enough relays and bridges upgrade, the many tens of thousands of Tor users in Iran will resume being able to reach the Tor network, without needing to change their software.

  How did the filter work technically? Tor tries to make its traffic look like a web browser talking to an https web server, but if you look carefully enough you can tell some differences. In this case, the characteristic of Tor's SSL handshake they looked at was the expiry time for our SSL session certificates: we rotate the session certificates every two hours, whereas normal SSL certificates you get from a certificate authority typically last a year or more. The fix was to simply write a larger expiration time on the certificates, so our certs have more plausible expiry times.

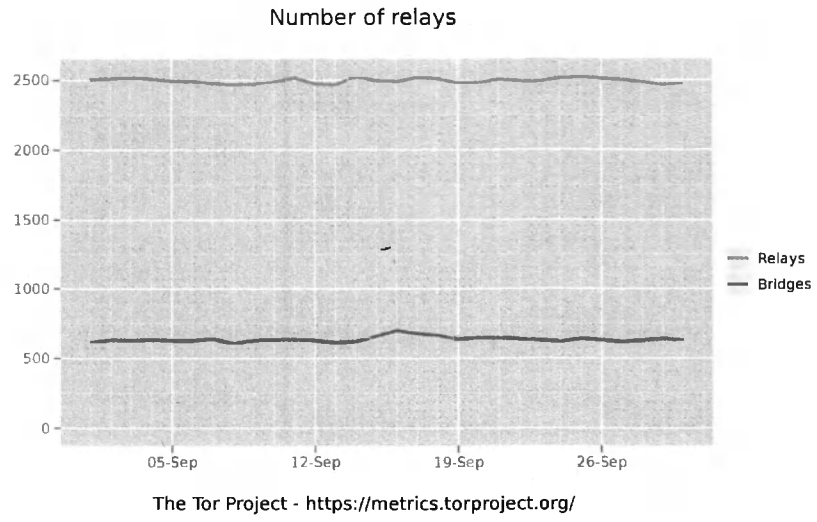
  See the full post at `https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fi`

Grow the Tor network and user base. Outreach.

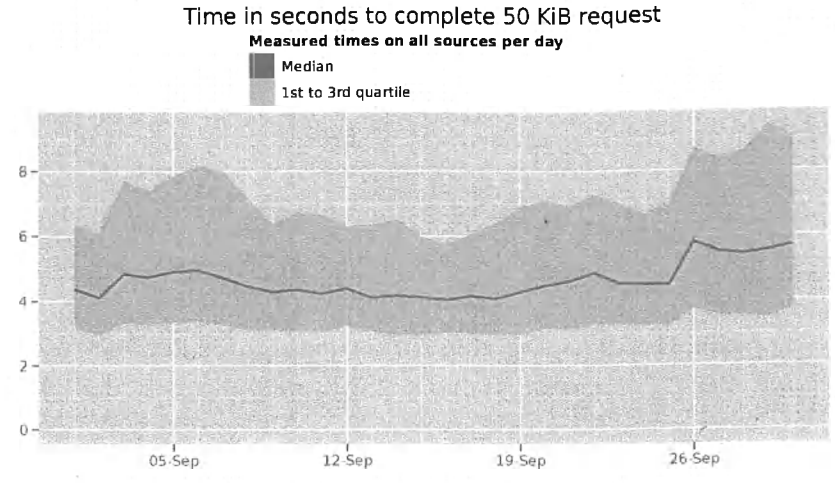
Measures of the Tor Network



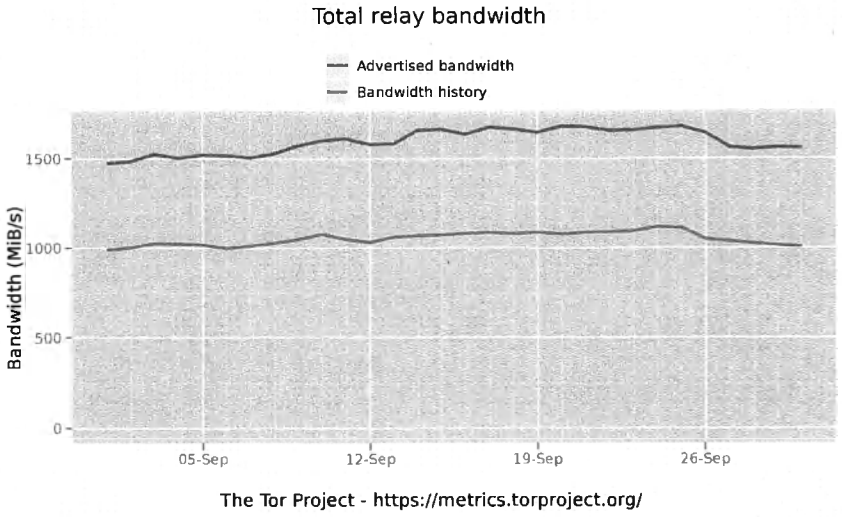
This graph shows the total quantity of exit relays in September 2011. There is a very slight reduction in relays over the month.



This graph shows the total quantity of relays and the total quantity of bridges in September 2011.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Average latency has increased slightly to 6 seconds at the end of the month. This is likely due to the loss of the four very-high bandwidth blutmagie exit relays.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The steady-state of relays creates almost 1.5GBps (12.0 Gbps) of bandwidth available.

Outreach and Advocacy

1. Jacob worked on the DigiNotar CA issues, https://blog.torproject.org/blog/diginotar-damage-discl You can see all of the issues related to DigiNotar at this url, https://blog.torproject.org/category/tags/ohdiginotaryoudidnt.
2. Jacob presented at a conference hosted by the Committee to Project Journalists, https://www.cpj.org/internet/2011/09/when-a-bug-fix-can-save-a-journalists-life.php#more.
3. Runa traveled to Ann Arbor to talk to Univerisity of Michigan about Telex and Tor.
4. Runa traveled to Los Angeles to help with a Persian News Network campaign to promote Tor.
5. Runa gave a talk about usability, security and Tor at Middlesex University in London.
6. Runa went to Hacks/Hackers London.
7. Andrew talked to the Florida Coalition Against Domestic Violence about data, network, and Internet security in the shelters. http://www.fcadv.org/.
8. Karen attended the United Nations Internet Governance Forum in Nairobi, Kenya. http://igf.or.ke/.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- Runa worked with some developers on finishing up an Amazon EC2/Cloud-based Tor relay image. http://torcloudservers.com/. This allows someone to simply use their AWS account to start up any number of Tor relay or bridge images.

Bridge relay and bridge authority work.

- Wrote a "Case study: Learning whether a Tor bridge is blocked by looking at its aggregate usage statistics, Part one." This was difficult to write, because we're lacking the data to say whether a bridge was in fact blocked or not. https://metrics.torproject.org/papers/blocking-2011-09-15.pdf

Scalability, load balancing, directory overhead, efficiency.

- Started reviewing the TorStatus code so that we can run it on yatei soon. We should take out some functionality that copies stuff that ExoneraTor and Metrics do better. Also, we need to fix a few bugs. Once that's done, we can deploy the new TorStatus as status.tpo.
- Rewrote large parts of ExoneraTor by creating a distinct database for it. The goal is to remove old non-aggregate data from the Metrics database. The new ExoneraTor allows searching for full days, not just timestamps, includes exit lists in its results, and can be extended to IPv6 quite easily once Tor supports it. Once I have some feedback saying the beta works for other people, I'll make it the new default. https://metrics.torproject.org/exonerator-beta.html

- Damian fixed some authentication bugs in TorCtl and arm, https://trac.torproject.org/projects/tor/ticket/3958.
- Juan Alcaine is helping with the arm RPMs, providing much needed testing and splitting arm from its dependencies. Next step is to get help from Erinn for uploading the arm/torctl rpms to the deb.tpo repos.
- Kamran has been working on a patch for exit locale selection in arm. It's functional, but not quite done yet.

Incentives work.

Nothing to report.

More reliable (e.g. split) download mechanism.

- Gettor updates to fix a number of bugs, updated text, and deployed the patches to production.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- Google Android's format is natively supported in Transifex, so we don't have to push and pull .po files for Orbot anymore (3987).
- Updated translations for the bridge db, gettor email system, vidalia, vidalia help files, vidalia installer, torbutton, and orbot.
- Updated translations in Arabic, German, Farsi, Hungarian, Spanish, French, Italian, Japanese, Korean, Swedish, Vietnamese, Polish, and Mandarin Chinese.
- At the end of September, after much discussion, we removed translated pages from the website. A full description of the change is available at https://blog.torproject.org/blog/whither-website-translations. We're working on a user manual that can be translated and included in documentation shipped with our software bundles.Of course, all of the software and related documentation will continue to be translated.

August 7, 2012

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #01:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 June 2012 - 17 July 2012	$25,000	$25,000
E013-12-IQ-00005-0	18 June 2012 - 17 July 2012	$39,633.35	$39633.35
Total Invoice		$64,633.35	$64,633.35

Thank you.

TorProject Invoice #BBG20120807

August 30, 2012

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #02:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 July 2012 - 17 August 2012	$25,000	$50,000
E013-12-IQ-00005-0	18 July 2012 - 17 August 2012	$39,633.35	$79,266.70
Total Invoice		$64,633.35	$129,266.70

Thank you.

TorProject Invoice #BBG20120830

September 28, 2012

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #03:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 August 2012 - 17 September 2012	$25,000	$75,000
E013-12-IQ-00005-0	18 August 2012 - 17 September 2012	$39,633.35	$118,900.05
Total Invoice		$64,633.35	$193,900.05

Thank you.

TorProject Invoice #BBG20120928

October 29, 2012

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #04:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 September 2012 - 17 October 2012	$25,000	$100,000
E013-12-IQ-00005-0	18 September 2012 - 17 October 2012	$39,633.35	$158,533.40
Total Invoice		$64,633.35	$258,533.40

Thank you.

TorProject Invoice #BBG20121028

November 28, 2012

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #05:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 October 2012 - 17 November 2012	$25,000	$125,000
E013-12-IQ-00005-0	18 October 2012 - 17 November 2012	$39,633.35	$198,166.75
Total Invoice		$64,633.35	$323,166.75

Thank you.

TorProject Invoice #BBG20121128